TECHNOLOGY FOR SECURE IDENTITY DOCUMENTS

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

OCTOBER 18, 2007

Serial No. 110–90

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.oversight.house.gov

U.S. GOVERNMENT PRINTING OFFICE

45–220 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

TOM LANTOS, California
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY MCCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho
JIM JORDAN, Ohio

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
DAVID MARIN, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
CAROLYN B. MALONEY, New York

BRIAN P. BILBRAY, California
TODD RUSSELL PLATTS, Pennsylvania,
JOHN J. DUNCAN, JR., Tennessee

MICHAEL MCCARTHY, *Staff Director*

CONTENTS

TECHNOLOGY FOR SECURE IDENTITY DOCUMENTS

THURSDAY, OCTOBER 18, 2007

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:05 p.m., in room 2247, Rayburn House Office Building, Hon. Edolphus Towns (chairman of the subcommittee) presiding.

Present: Representatives Towns, Welch, and Bilbray.

Staff present: Michael McCarthy, staff director; Cecelia Morton, clerk; and Charles Phillips, minority counsel.

Mr. TOWNS. The hearing will come to order.

Today's hearing will examine the important topic of how to make a secure identification card. On issues like identity theft, immigration and homeland security, there have been repeated calls for a secure or a tamperproof ID. I have heard a lot of discussion but have been short on details. How do you make an ID tamperproof? What is the tradeoff between security and privacy? How much is it going to cost?

I hope we can answer some of those questions today. After all, this is an issue that affects everyone in this country. Whether you are trying to board a plane, cross the border or fill out your payroll forms, you will be asked for identification. We have to make sure this ID can't be forged or misused, and we also have to make sure that we respect privacy and spend efficiently.

One of the problems is that there are so many forms of ID issued by different parts of the Federal and State governments. This issue came up for me recently when I was at the airport in Orlando, FL, going through security. They asked me for my ID. So, I showed them my congressional ID, and they said, "No, we don't take that here. You can't go through here with that." So, fortunately, a supervisor with some understanding and, maybe, sense was daring to let me go through, but it highlights the need for more consistency in how ID cards are recognized.

There are a lot of reasons not to have a national ID card, but what I think we do need are some common standards so that airport screeners or police officers can easily tell whether an ID is legitimate. I think we can also eliminate the overlap between some of these programs, both to save the government some money, and also so that people don't have to carry around so many cards.

I see plenty of overlap out there. GHS has three different programs issuing cards to frequent border crossers. The Federal Government is issuing SmartCards to its employees and contractors under the HSPD–12 program and is issuing SmartCards to transportation workers under an entirely separate program. There have been some efforts to combine programs, which is a good step.

The director of the Vermont Department of Motor Vehicles is here today to discuss Vermont's plan to issue a combined driver's license and border crossing card. Our witnesses today will also talk about advanced ID technology like SmartCards and radio frequency identification. These technologies can increase security, but it comes at a cost. Not only are the cards more expensive, but they require a whole infrastructure of data bases and readers to be used to their full potential.

The Federal Government is promoting these SmartCard programs, and I'd like to hear whether this is something the States should be doing as well. Also, I'm worried that all of the security is going into the chips, so if the computers don't work and the cards are checked by hand, they could actually provide less security. That is a real concern.

Overall, I hope today's hearing will put into focus the policy decisions that need to be made about ID cards: balancing security, cost, and privacy. We are building a record on these issues because they are not going away any time soon, and I think we are all agreed to that.

[The prepared statement of Hon. Edolphus Towns follows:]

OPENING STATEMENT
OF
CHAIRMAN EDOLPHUS TOWNS

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

HEARING ON TECHNOLOGY FOR SECURE ID CARDS
October 18, 2007,
2:00 p.m. 2247 Rayburn

Today's hearing will examine an important topic – how to make a secure identification card. On issues like identity theft, immigration, and homeland security, there have been repeated calls for a secure or tamper-proof ID. However, a lot of this discussion has been short on details. How do you make an ID tamper-proof? What is the tradeoff between security and privacy? And how much is all this going to cost? I hope we can answer some of those questions today.

After all, this is an issue that affects everyone in this country. Whether you are trying to board a plane, cross the border, or fill out your payroll forms, you will be asked for ID. We have to make sure that this ID can't be forged or misused, and we also have to make sure we respect privacy and spend efficiently.

One of the problems is that there are so many forms of ID, issued by different parts of the federal and state governments. This issue came up for me recently, when I was at the airport in Orlando going through security. They asked me for ID, so I showed them my Congressional ID. They told me we don't take that kind of ID. Fortunately, a supervisor with some common sense was there and let me go through, but it highlights the need for more consistency in how ID cards are recognized.

There are a lot of reasons not to have a national ID card, but what I think we do need are some common standards, so that an airport screener or police officer can easily tell whether an ID is legitimate. I think we can also eliminate the overlap between some of these programs, both to save the government some money, and also so people don't have to carry around so many cards.

I see plenty of overlap out there. DHS has three different programs issuing cards to frequent border crossers. The federal government is issuing smartcards to its employees and contractors under the HSPD-12 program, and is issuing smartcards to transportation workers under an entirely separate program. There have been some efforts to combine programs, which is a good step. The Director of the Vermont Department of Motor Vehicles is here today to discuss Vermont's plan to issue a combined driver's license and border crossing card.

Our witnesses today will also talk about advanced ID technology like smartcards and radio frequency identification (RFID). These technologies can increase security, but it comes at a cost. Not only are the cards more expensive, but they require a whole infrastructure of databases and readers to be used to their full potential. The federal government is promoting these smartcard programs, and I'd like to hear whether this is something the states should be doing as well. Also, I'm worried that all the security is going into the chips, so if the computers don't work and the cards are checked by hand, they could actually provide less security.

Overall, I hope today's hearing will put into focus the policy decisions that need to be made about ID cards – balancing security, cost, and privacy. We're building a record on these issues, because they are not going away anytime soon.

***

Mr. TOWNS. I now recognize the ranking member of this subcommittee, the gentleman from California, Mr. Bilbray.

Mr. BILBRAY. Thank you very much, Mr. Chairman.

First of all, Mr. Chairman, I'd ask that I be allowed to introduce the gentleman from Ohio to introduce his testimony on this item.

Mr. TOWNS. Without objection.

Mr. BILBRAY. Mr. Chairman, let me first thank you very much for holding this hearing but not just this hearing. I want to make a public statement that I may regret in the future, but I am very proud to serve with you on this committee. With all the talk around this country of why there aren't more bipartisan efforts made for the good of America in Washington, I think your committee is a shining star we can use as an example, and I challenge anyone to show me anybody in Washington who works as bipartisan for the common good as your committee does. I want to thank you for that, and that really reflects your leadership and your personal commitment to caring more about outcome than partisan advantage, and I want to say that publicly.

Mr. TOWNS. Thank you.

Mr. BILBRAY. The other issue, Mr. Chairman, as somebody who comes from local government and in the 5-year sabbatical that the voters gave me in the early days, as my kids say, I was able to work on the REAL ID bill with both sides of the aisle. The one thing that, I think, we learned was that there was not a conflict between privacy and security. In fact, there can be no secure privacy without a secure system. History has shown that the greatest violation of privacy is when people are able to steal someone's ID, be it name, be it Social Security number or other, and not have a system where they get caught because we do not have a secure identification system that is able to block the repetitive use of somebody's identity. Ask anyone who has been a victim of that, of identity theft. It would sure be nice to have a secure system that the hackers can't get into.

Just to reflect on the commonality of our efforts here between the Chair and the ranking member, Mr. Chairman, just this week, the security guards at Fort Belvoir did not want to recognize my congressional ID at a military installation, mostly because, they say, "We've never seen it before." So I think that this is an effort of looking at the best available technology and how we can move forward.

Let me just say this as a challenge to those of us who are in the system: as somebody who has been in government ever since I was 25 years old as a city council member, those of us in government really need to look at the private sector with their breakthrough, but as has been said before, doggone it, if we can go anywhere in the world, Mr. Chairman, anywhere in the world, take a card, stick it in, punch a couple of numbers and that little machine in El Salvador or in Russia knows how much money we have in what bank and where and can get us our money out, if that can work anywhere in the world, doggone it, we should be able to have a system that works here in the United States.

It is a challenge for us to say how we can improve on that and build on that, so I look forward as this being the first step of a very, very aggressive policy. Since 9/11, I think we all agree we

haven't done enough in this field. We need to do more. The 9/11 Commission said quite clearly this was a critical component that was lacking and that needed to be filled, and hopefully, in working with your leadership, Mr. Chairman, we will be able to fulfill that mandate from the 9/11 Commission for the good of the American people.

I yield back.

Mr. TOWNS. Thank you very much, and also, thank you for your kind words as well. Thank you.

At this time, I yield to Congressman Welch.

Mr. WELCH. Thank you very much, Mr. Chairman and ranking member.

You know, this is my first time in Congress, and I used to watch on C–SPAN when Members of Congress would give their statements and brag about their colleagues from their home States, and I'm getting a chance to do it.

Bonnie Rutledge is the Commissioner of Motor Vehicles in Vermont, and I really am proud of her. She runs the department. She has been, really, a lifelong career public servant. Everybody who has a problem calls her, from the Governor to my next-door neighbors, and Vermont is kind of a small place, 650,000, Mr. Chairman, and I know you're from a State that has a few more people than that, and in our State——

Mr. BILBRAY. How many people in the State?

Mr. WELCH. 650,000, and Bonnie knows them all, and I'm not kidding. I was late one time filing for my driver's license, and I think Bonnie called me up and asked me if I'd forgotten to do something, so we get good service.

This topic is so important, the secure IDs, but also in Vermont, along with a lot of the northern border States, we have these extraordinary relationships with our friends in Canada, and it ranges from business—Canada is our second largest trading partner or, I guess, the largest trading partner, and there's commerce back and forth.

We've got one house up in northern Vermont that is partly in Vermont and partly in Canada. We have kids who play on hockey teams up there, and they're back and forth all the time for their little league hockey games. We have to find some practical way that doesn't compromise those good relationships that we have with Canada, both economic and social, and Bonnie Rutledge is at the forefront of doing that.

So I'm very grateful to your services. It is really nice of you to come down here and give us the benefit of your years and experience.

Mr. Chairman, I really thank you.

Mr. TOWNS. Thank you. Thank you very much.

Before we get started, we want to ask our witnesses to stand. We swear our witnesses in here.

[Witnesses sworn.]

Mr. TOWNS. Let the record reflect that all of the witnesses answered in the affirmative.

Let me introduce our first panel. Kathy Kraninger is the Director of the Screening Coordination Office at the Department of Home-

land Security where she is responsible for coordinating DHS' identification program.

Welcome. We are delighted to have you.

Benjamin Brink is the Assistant Public Printer for Security and Intelligent Documents at the Government Printing Office. Mr. Brink is also a captain in the Navy Reserve and has been called up to serve in Afghanistan in the coming year.

Welcome, and we thank you for your service both in terms of our country and, of course, for the Printing Office as well.

David Temoshok is the Director for Identity Policy and Management for the Office of Government-wide Policy at the General Services Administration.

Welcome.

Finally, Bonnie Rutledge, who has already had an introduction, and of course, I will want to give her another one as well. She traveled all the way from Vermont, as you heard, to be with us today, where she is the director of the Vermont Department of Motor Vehicles.

Your entire statements, everybody, will be in the record, so I will ask each witness to summarize their testimony within the time we have established for each of you, which is 5 minutes. Now, first, there will come a yellow light that says, you know, "caution," and then all of a sudden, there will come a red light. When that red light comes on, that means "stop," you know, and of course, remember the procedure—green, yellow, red.

OK. Thank you very much.

You may start, Ms. Kraninger.

STATEMENTS OF KATHY KRANINGER, DIRECTOR, SCREENING COORDINATION OFFICE, U.S. DEPARTMENT OF HOMELAND SECURITY, ACCOMPANIED BY MICHAEL EVERITT, DIRECTOR, FORENSIC DOCUMENT LABORATORY, IMMIGRATION AND CUSTOMS ENFORCEMENT, U.S. DEPARTMENT OF HOMELAND SECURITY; BENJAMIN BRINK, ASSISTANT PUBLIC PRINTER FOR SECURITY AND INTELLIGENT DOCUMENTS, GOVERNMENT PRINTING OFFICE; DAVID TEMOSHOK, DIRECTOR, IDENTITY POLICY AND MANAGEMENT FOR THE OFFICE OF GOVERNMENT-WIDE POLICY, GENERAL SERVICES ADMINISTRATION; AND BONNIE RUTLEDGE, DIRECTOR, VERMONT DEPARTMENT OF MOTOR VEHICLES

STATEMENT OF KATHY KRANINGER

Ms. KRANINGER. Good afternoon, Mr. Chairman, Congressman Bilbray and Congressman Welch. It is a pleasure to be here today and to represent the Department of Homeland Security.

We do have a number of ongoing efforts to secure identification documents, thereby improving the way we screen people and process them through our operations. Identity documents provide one means of demonstrating with varying levels of assurance that individuals are who they say they are, and as such, they form the basis of this screening process.

It is worth noting that Secretary Chertoff established my office, the Screening Coordination Office, to integrate DHS screening and credentialing activities. We recognize many of the efforts that you

have noted do seem to be either disaligned or not rationalized and focused, and for that reason, we want to make sure that our efforts are enhancing our missions to keep dangerous people and goods out of the United States and to secure critical infrastructure. Many of you are very familiar with our operations, but it certainly helps sometimes to hear it in numbers terms.

Customs and Border Protection admits 420 million people to this country every year, 88 million of them by air alone. Every day, as Chairman Towns knows, too, we process through TSA screening checkpoints nearly 2 million people, and every year, U.S. Citizenship and Immigration Services processes 7 million immigration benefits applications, so we do encounter a number of individuals through our processes as well as the requirements that have come down since September 11th for critical infrastructure workers, with the transportation workers' identification credentials. With the chemical sector security law, as well, that passed, there are a number of critical sectors that are covered, and those individuals have to undergo background checks that are done at the Federal level. So these are all programs that are based around identity, and that may result in the issuance of a credential.

So, given the number of individuals that DHS encounters every day, we are constantly evaluating and improving our processes and asking ourselves "How do we effectively process these travelers and these applicants while identifying those among them, the very small percentage among them, who present a threat?" and more specifically, "How do we deter or intercept terrorists who are willing to die for their cause? How do we do that without unduly impacting the lives of everyone else or without bringing trade and travel to a screeching halt?"

As you noted, Congressman, the 9/11 Commission pressed the importance of this issue, "Sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists," and also, "For terrorists, travel documents are as important as weapons."

Indeed, when we investigated the 9/11 attacks, we discovered that 18 of the 19 perpetrators had been issued U.S. identification documents and that some of these documents had been obtained fraudulently, and many of those were driver's licenses and, in fact, a number of driver's licenses held by each individual.

As noted, DHS does have a number of high-profile screening programs that are underway, and what needs to be pressed is that the business case for these programs drives the technology decisions that are made. You will hear today from a number of witnesses—the colleagues on this panel who produce a number of documents even for the Department of Homeland Security, the State of Vermont that is in a partnership with us to produce an Enhanced Driver's License and is committed to implementing, potentially, REAL ID and, as well, the second panel that will cover a number of physical security features that are critical to securing the document, itself.

My statement notes some of those things, and I can certainly, in questions, go into the features that are in the documents that DHS issues, but in the interest of time and recognizing the chairman's note about 5 minutes, I will not go into that at this time. I will,

however, make the case, at least, for one key program area, and again, we are using a number of different technologies based on the business cases presented.

So, with one example in my oral statement and the rest in my written, I would like to talk about, very briefly, the Western Hemisphere Travel Initiative [WHTI].

WHTI requires the institution of a secure document that denotes identity and citizenship, for entering the United States right now through land and sea ports of entry. Today, we do not have a document requirement, though, certainly CBP officers, Customs and Border Protection officers, are requesting some demonstration of identity and citizenship for most individuals who enter the land border but not all. We see over 8,000 different documents, and CBP officers have the challenge of determining which are legitimate and which are not today.

This is a huge challenge to law enforcement and to these officers, and from a business standpoint, DHS is faced with the challenge of determining whether or not these individuals should enter the United States, and it is, roughly, 1 million people a day. Recognizing that at the same time we face this security imperative, we have to deal with the facilitation of that legitimate trade and travel. So, from that standpoint, we have made a choice with respect to technology that will enable us to meet our security mission and this facilitation need, and that's the use of vicinity RFID technology, building upon our trusted traveler programs that, today, involve 300,000 people who cross the border and who use those cards successfully.

So that's just one example of one of the business and technology decisions that we have made, and we have others, and I'm happy to take questions from you as we get to that point in the hearing.

Mr. TOWNS. Thank you very much for your testimony.

[The prepared statement of Ms. Kraninger follows:]

UNITED STATES DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF KATHLEEN KRANINGER
DIRECTOR, SCREENING COORDINATION OFFICE

Before the

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND
GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
ORGANIZATION, AND PROCUREMENT

October 18, 2007

Good afternoon Chairman Towns, Ranking Member Bilbray, and distinguished members of the Subcommittee. Thank you for this opportunity to discuss the ongoing efforts of the Department of Homeland Security (DHS) to secure identification documents, thereby improving the way we screen and process people. Identity documents provide one means of demonstrating, with varying levels of assurance, that an individual is who they say they are. As such, they form the basis of the screening process. The ability to quickly and accurately confirm a person's identity and check it against watch lists to identify potential hostile intent is crucial to the Department's mission.

The Screening Coordination Office, which I direct, was established by Secretary Chertoff last summer to integrate, where appropriate, DHS screening and credentialing activities to enhance our missions of keeping dangerous people and things out of the U.S. and securing critical infrastructure. To give you an understanding of the security challenge we face in the United States, let me paint a picture of DHS operations.

Each year, Customs and Border Protection (CBP) admits approximately 420 million travelers– 88 million by air alone. In any given day, the Transportation Security Administration (TSA) screens over 2 million passengers using our domestic U.S. aviation system; and we rely on state and local partners to patrol surface transport, which handles traveler volumes that far exceed these levels. Each year U.S. Citizenship and Immigration Services (USCIS) processes nearly 7 million immigration benefits applications and petitions for foreign nationals. How do we effectively process travelers and applicants while identifying those among them who present a threat? More specifically, how do we deter or intercept terrorists who are willing to die for their cause – and how do we do that without unduly impacting on the lives of everyone else or bringing trade and travel to a screeching halt?

The National Commission on Terrorist Attacks Upon the United States, also known as the 9-11 Commission, pressed the importance of secure identification documents that can be verified in the screening process. "[S]ources of identification are the last opportunity

to ensure that people are who they say they are and to check whether they are terrorists." "For terrorists, travel documents are as important as weapons." Indeed, when we investigated the 9/11 attacks, we discovered that 18 of the 19 perpetrators had been issued U.S. identification documents and that some of these documents had been obtained fraudulently.

The need for secure identification is clear, but how should we determine what level of identity assurance is appropriate for a given encounter? Should biometrics be collected? Must the document be electronically verifiable?

Mission and Business Case Must Drive Technology Decisions

The business process and needs of our screening efforts must drive the technology choices that we make for our secure identification programs. We are fortunate to have many technology options today to choose from. These technologies supports our ability to: establish and verify the identity of individuals, both at time of enrollment and at subsequent encounters; conduct vetting appropriate to determine eligibility and assess risk for the specific program, including conducting checks against the Terrorist Screening Database (TSDB); assess validity of documents presented, as well as using physical security features to ensure documents are tamper-resistant. It is important to understand that, because the vetting conducted by DHS in a given program is based on the requirements of the program, an individual who has successfully completed a background check for one type of credential cannot be automatically qualified for other credentials if the vetting for that program is more stringent.

DHS is currently developing and implementing a number of high profile screening programs in which secure identification credentials figure prominently. As DHS develops the path for these programs, it creates its business case, unique to that program. This business case includes: the use case or business process desired; analysis of the environment in which the process will occur; the requirements established by the enabling legislation and the authority for the program; the overall mission of the implementing organization as well as DHS as a whole; the risks associated with the process or program; and mechanisms to ensure the protection of privacy and civil rights concerns.

While recognizing the individual challenges and environments, we must also identify opportunities to harmonize and enhance screening processes across DHS programs and rationalize and prioritize investments in screening technologies and systems. DHS has adopted the following principles to guide development of screening programs, where appropriate.

- Design credentials to support multiple licenses, privileges, or status, based on the risks associated with the environments in which they will be used.
- Vetting, associated with like uses and like risks, should be the same.
- Immigration status determinations by DHS components should be verified electronically.
- Eligibility for a license, privilege, or status should be verified using technology.

- Design enrollment platforms and data collection investments so that they can be reused by other DHS programs – establishing a preference for "enroll once, use many" environment, where appropriate.
- Ensure opportunities for redress – individuals should be able correct information held about them.

While one size does not fit all, neither does every program have to reinvent the wheel.

The following programs provide examples to illustrate how different the technology solutions can, and should, be when they are chosen to respond to business needs.

Western Hemisphere Travel Initiative (WHTI)
The institution of a travel document requirement and the standardization of travel documents are critical steps to securing our Nation's borders and increasing the facilitation of legitimate travelers. Currently, travelers at our land and sea ports of entry may present any of 8 thousand documents to CBP officers when seeking admission to the United States.

Our layered security strategy involves identifying and interdicting terrorists as early as possible – if not before they enter our country, then at the port of entry. Through its requirement that individuals carry a passport or other acceptable secure document to denote identity and citizenship, WHTI will greatly reduce the opportunities for fraud or misrepresentation of one's identity.

DHS has proposed accepting the cards associated with the existing trusted traveler programs, NEXUS, SENTRI, and FAST, and expanding the use of the facilitative technology already in use in these programs, vicinity Radio Frequency Identification (RFID), to other documents. This technology allows a unique card identifier to be read as the driver approaches the inspection booth, and the record associated in the system with that card is presented for the CBP Officer. The Department of State's Passport Card, currently under development, will also use vicinity RFID technology to meet DHS' operational needs at ports of entry. NIST certified the card architecture of the passport card as required in the FY 2007 DHS Appropriations Act.

Speeding up the document querying and authentication process gives more time for our CBP officers to ask questions and conduct inspections of those who require more scrutiny. Precious time now spent examining the face of a document will, instead, be used to interview higher risk individuals seeking to enter the U.S. We believe that with more people having secure documents and using this technology, WHTI will improve traffic flow at the border.

Because these documents will be used by DHS to determine eligibility to enter the U.S., and can directly interact with DHS systems, we can minimize the information on the document and rely instead on the information contained in DHS systems to verify that the person presenting the document is the one to whom it was issued.

In contrast, the business process associated with the Transportation Worker Identification Credential (TWIC), and the environment in which it's used, differs significantly.

Transportation Worker Identification Card (TWIC)
In furtherance of securing our seaports, the TWIC is a DHS screening initiative with joint participation from the TSA and the U.S. Coast Guard. The TWIC program, which began its roll out this week, provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities and vessels regulated under the Maritime Transportation Security Act of 2002. National deployment of the TWIC program will enhance security of ports by requiring credentialed merchant mariners and workers with unescorted access to secure areas of vessels and facilities to undergo a complete security threat assessment, which includes a fingerprint-based criminal history records check, and receive a TWIC.

In the future, port facility and vessel owners and operators will be required to integrate TWIC into their existing access control systems and operations. This second phase of the program will implement card reader requirements through rulemaking to verify the identity of workers entering secure areas by matching their fingerprint with the fingerprint template stored on their TWIC. Before implementing these requirements, DHS will conduct pilot tests in accordance with the SAFE Port Act, and the public will be afforded ample opportunity to comment on that aspect of the TWIC program through the rulemaking process.

The TWIC is intended to be used in a highly decentralized environment for biometric-based automated access control. Because of this, personally identifiable information must be included on the card that allows the reader technology, without human intervention, to make the determination as to whether the person presenting the document is the one to whom it was issued and whether the card is currently valid. In this program, decision-making for initial or continued eligibility, as well as issuance of the TWIC document, is centralized and determined through human review. The environment in which the TWIC is used, however, is decentralized and automated.

In a third contrast, the business process associated with the REAL ID program provides another aspect of this discussion.

REAL ID
During the terrorist attacks on the United States on September 11, 2001, all but one of the terrorist hijackers acquired some form of identification document, and used these forms of identification to assist them in boarding commercial flights, renting cars, and other necessary activities leading up to the attacks.

In response to the 9/11 Commission's recommendations, in May 2005, Congress enacted the REAL ID Act. The REAL ID Act directs DHS to establish certain minimum standards that States must adopt for State issued driver's licenses and identification cards intended for use for Federal official purposes, including access to federal facilities,

boarding Federally-regulated commercial aircraft, entry into nuclear power plants, and such other purposes as established by the Secretary of Homeland Security.

It is important to reiterate that this program will establish a set of minimum standards. The role of the Federal government in this case is to ensure commonality of approach, which includes minimum physical security features as well as quality and integrity of the issuance process, because of the role driver's licenses play in the U.S. as a core identity document. At the same time, we recognize that individual States have a strong and continuing interest in ensuring that these documents meet their primary purpose – the ability for the State to ensure and enhance driver safety.

Identification documents complying with the REAL ID Act are intended to be issued and used in a highly decentralized environment, with a variety of different users and business processes. Many of the users may not have rapid and easy access to automation from which to verify the authenticity of the document or verify that the person who presents the document is the one to whom it was issued. In this program, State driver's license eligibility determinations are informed and supported by electronic verification of the supporting documentation presented by the applicant with the agency who issued it. Use and validity of the document remains highly decentralized and usually requires human verification at the point where an individual is using a REAL ID driver's license or identification card as an identity document.

Privacy Considerations

In leveraging technologies for border security and facilitation of legitimate global travel, DHS has institutionalized the need to protect privacy, and is committed to adhering to the strictest privacy standards. DHS only collects information needed to achieve the program objectives and mission and only uses this information in a manner consistent with the purpose for which it was collected. DHS conducts periodic audits of its systems to ensure appropriate use. In addition, DHS provides notice regarding how information collected will be used and shared with outside entities, and how the information will be securely stored. DHS also provides notice to the individuals who participate in the programs as to the objectives and benefits of the program, as well as the privacy risks. These are the privacy principles that provide the opportunity for informed consent.

Analysis of risks to privacy and the manner in which those risks can be mitigated also plays a key role in determining which technologies will be used, and how, for a given mission. For example, the business case for WHTI documents the need for CBP to rapidly verify that the person presenting the document is the one to whom it was issued, that the document is valid, and to use information about that person to conduct appropriate checks. Vicinity RFID was selected as the technology best able to meet these requirements, because of its ability to be read at a distance and without close interaction with the card holder. DHS assessed the privacy risks associated with vicinity RFID, and has made technology choices to mitigate those risks. The vicinity RFID on the WHTI compliant document will only transmit a randomly assigned number to CBP's systems, and will not include any personally identifiable information. CBP's systems will then provide the information needed about the person to the officer for the encounter. This

mitigates the risk that an unauthorized person would intercept the RFID transmission and obtain meaningful information. The privacy risks were similarly assessed and mitigated in the implementation choices for the technology selected for the TWIC and REAL ID programs.

Physical Document Security Requirements

Physical security features are required on secure identification documents so the document can be used for its intended purpose when electronic verification systems are not available. Documents must be made physically secure using layered multiple security features, such as holograms, kinegrams, specialized inks, laser etching, and new security printing techniques specifically designed to thwart attempts to counterfeit or alter the documents.

To maintain a high level of physical document security, both to allow for secure processes and to protect the privacy of the individual, document producers and those who issue legitimate documents are in a constant battle to develop new production methods and security features to make the identification documents they issue more secure. However, technological advances have made commercial-quality scanning and printing equipment and processes widely available to the individual consumer. The availability of commercial-quality scanning and printing equipment and processes has significantly increased the quality of fraudulent documents encountered by all levels of law enforcement and government agency personnel.

It is for these reasons that access, travel, and identity documents must be continually reviewed and updated. The documents must incorporate advances in production technology and security features specially designed to thwart reproduction by scanners or other digital equipment. These investments will produce documents that are more tamper-resistant and therefore more secure. The development, production, and distribution of quality physically secure documents will be expensive, as it will require replacing old document production systems and infrastructure; however, the investment will pay healthy dividends in the security of this country.

Summary

These examples demonstrate the rationale for advocating a process whereby the business needs drive the technology appropriate for a specific use environment. I would like to also underscore how important it is that the DHS, charged with implementing these programs, continue to have the flexibility to analyze the program's requirements, and select the technology that best meets the needs of the environment. Mandates to use a specific technology would not permit DHS to utilize the most appropriate approach for a given mission, and would restrict our ability to evolve that approach in response to changing threats. This does not mean that DHS believes that every program should use a different technology solution. DHS is moving to standardize to a select few solutions, appropriate to the environments in which they will be used and the mission need of the program.

Mr. Chairman, thank you again for the opportunity to testify today. I am happy to respond to the Subcommittee's questions.

Mr. TOWNS. Mr. Brink.

STATEMENT OF BENJAMIN BRINK

Mr. BRINK. Thank you, Mr. Chairman, Congressman Bilbray and Congressman Welch, for inviting the Government Printing Office to appear here today to discuss technology for secure identity products.

I am Ben Brink, Assistant Public Printer for Security and Intelligent Documents. As the chairman mentioned, I'm soon off to Afghanistan and so won't be available for follow-on questions.

If I may introduce my colleague behind me, Reynold Schweickhardt, who is the Chief Technology Officer for GPO, he can be available to you or your staff for any followup.

Before receiving my orders, I headed GPO's Security and Intelligent Documents' Business Unit, which was formed to produce the electronic passport, or e-Passport, for the State Department and to produce other Federal products containing both print and electronic security measures.

GPO has been the government's printer for more than a century. Today, our fastest growing product line is Security and Intelligent Documents. We've produced these documents in a trusted, government-controlled environment, using a secure supply chain, secure technology and secure personal information.

As of this date, the e-Passport represents the majority of our business; although, we project a growing business in SmartCards and other secure identification documents. We have recently received a requisition for SmartCards from the Department of Homeland Security. GPO has been producing passports since 1926. Today's passport resulted from a 2001 standard issued by the International Civil Aviation Organization. Development was underway at the time of 9/11 and has accelerated quickly afterwards. The first U.S. e-Passport was issued to the Secretary of State in 2005, and GPO completed its conversion to e-Passport production in May 2007. Today, more than 15 million U.S. e-Passports have been issued, more e-Passports than all other nations combined, and GPO is currently producing more than 550,000 per week to meet unprecedented citizen demand.

The principle behind securing the e-Passport is a series of layered features, including numerous overt and covert physical features embedded in the design, print, chemistry, paper, inks, and threads of each passport page. In addition, electronic security features are embedded in each e-Passport, using an integrated circuit. This chip, designed, tested and proven secure under the most challenging conditions, contains the same personal information that is printed on the data page of the Legacy Passport, including a digital photograph.

I've brought samples of these products for question time, and can make those available to the committee.

Our e-Passport program has given us expertise to create an expanding family of e-credentials, using proven e-Passport physical design and electronics. We are now assisting Federal agencies in meeting the requirements of HSPD–12 and other Federal SmartCard programs.

SmartCards use the same principle of layered security adapted for plastic materials. SmartCards are composed of layers of material with both printed features and a programmable chip and antenna. In addition to designing SmartCards, GPO is procuring the capability to personalize SmartCards, the process by which the personalized data is printed on the SmartCard, and its chip is programmed with identity information, biometric data and permissions.

Today, GPO has designed the security printing for two card-based identification systems—the most recent, the Trusted Traveler, the SENTRI and the NEXUS cards—for the Department of Homeland Security. Again, I have a picture of that which I can show you later. It confirms identity and speeds border crossing for our preregistered travelers between the United States, Canada and Mexico. GPO has also designed the artwork in nonelectronic security features for the new Department of Defense Common Access Card [CAC], and I have a sample of that as well. It is the ID card which is used for all U.S. service personnel. This card provides both visual and electronic identification as well as physical and logical access to buildings and systems using its electronics. GPO has also assisted the Social Security Administration in designing the new security features of its new nonelectric Social Security Card.

When a SmartCard is read, the transmission of the identity information is often protected by a Public Key Infrastructure encryption, ensuring the highest level of protection for electronic information. GPO has recently been designated as a Shared Services Provider for PKI, one of the two civilian agencies with that designation.

Our Security and Intelligent Documents' consulting and design services have been sought by the State Department, the Department of Defense, the Department of Homeland Security, the FBI, the Coast Guard, and the Social Security Administration. We have also made recommendations to the REAL ID Standards Committee, participating through the Document Security Alliance where one of our security document experts sits on the board. GPO adds value to our consulting services by guiding policy formulation in organizations focused on national document policy.

Mr. TOWNS. Thank you very much, Mr. Brink, for your testimony.

[The prepared statement of Mr. Brink follows:]

Benjamin M. Brink
Assistant Public Printer for Security
and Intelligent Documents
Government Printing Office

Prepared Statement Before the Subcommittee on Government Management, Organization, and Procurement

Committee on Oversight and Government Reform House of Representatives

On Technology For
Secure Identity Products

Rayburn House Office Building, Room 2247

Thursday, October 18, 2007
2:00 PM

U.S. GOVERNMENT PRINTING OFFICE KEEPING AMERICA INFORMED
www.gpo.gov

Mr. Chairman and Members of the Subcommittee, thank you for inviting the Government Printing Office (GPO) to appear here today to discuss technology for secure identity products.

I am Benjamin M. Brink, Assistant Public Printer for Security and Intelligent Documents. Until recently when I was recalled to active duty to mobilize to Afghanistan, I headed GPO's Security and Intelligent Documents business unit, which was created last year as part of our *Strategic Vision for the 21st Century* (December 2004), to perform the functions necessary to produce the e-Passport for the State Department and other Federal products containing both print and electronic security measures.

By both law and tradition, GPO — an agency of the legislative branch – has three essential missions: to provide expert publishing and printing services to all three branches of the Federal Government; to provide, in partnership with Federal depository libraries, permanent public access to the printed and electronic information products of the Government; and to sell copies of authentic printed and electronic documents and other Government information products to the general public.

GPO currently employs about 2,300 staff, more than 75% of whom are represented by 10 unions with 15 bargaining units. For FY 2007, GPO had a total budget of $888 million. Approximately $120 million of that came from direct appropriations for Congressional Printing and Binding and for the Superintendent of Documents. The vast majority of our budget is derived from selling products and services to the Federal Government and the general public.

E-Passports Recently, GPO's fastest growing products and services have been security and intelligent documents. We produce these documents in a trusted, Government-controlled environment, using a secure supply chain, secure technology, and secure personal information. At this date, e-Passports represent the majority of this business, although we project a growing business in Smart Cards and other secure identification documents. We recently received a requisition for Smart Cards from the Department of Homeland Security.

GPO has been producing passports since 1926, when the League of Nations created an international standard for a booklet-style passport specifying the size of the booklet, the position of type, and the method of binding the cover to the pages. Because of GPO's expertise in precision printing and binding, we were selected to produce all passports and we've had the job ever since. Throughout that period, with the State Department and other security agencies, GPO has continuously improved the security of the world's most respected travel document.

Today's e-Passport is the result of a standard issued in 2001 by the International Civil Aviation Organization (ICAO), a bureau in the United Nations that sets standards for many aspects of air travel, including the international standard for interoperable e-Passports. Developmental work was underway at the time of 9/11 and accelerated quickly afterwards. The first U.S. e-Passport was issued to the Secretary of State in 2005.

The principle behind securing the e-Passport is in layered security features. The intricate design of each e-Passport page is in itself a security feature. GPO designers are trained and certified to use secure software to create these designs. Other features are not visible to the naked eye. The security fibers woven into passport paper, and the glue that reinforces the booklet stitching, can only be viewed under ultraviolet light.

Another deterrent to counterfeiting is a sandwich of layered transparent film encasing each data page. On this page, a traveler's identity information and photograph are displayed. Once the layers are fused together, any attempt to separate the layers will destroy all of them. On one of the layers, a kind of super-hologram is embedded. Its appearance changes under fluorescent light from a seal, to a profile of Benjamin Franklin, then to the letters "USA." There are multiple other security features in the pages of the e-Passport booklet.

At the heart of every e-Passport is an integrated circuit, or chip. The chip has been designed, tested, and proven secure under the most challenging conditions. It contains the same personal information that is printed on the data page of the old passport. The only new item is a digital photograph in place of a traditional one. E-Passports are identifiable by the biometric logo stamped on the cover.

Following the issuance of the first e-Passport, there was a dramatic ramp up in e-Passport production during 2006, while production of the non-electronic, or legacy, passport continued. By March 2007, e-Passport production exceeded that of legacy passports, and production of legacy passports ceased altogether in May 2007. Since then, all passports manufactured are e-Passports.

A total of 25 countries currently issue e-Passports that are compatible with the ICAO standard. With more than 15 million e-Passports issued to date, the U.S. has issued more e-Passports than all other nations combined and is currently producing more than 550,000 per week to meet unprecedented citizen demand. GPO manufactures three kinds of e-Passports: Tourist, Diplomatic, and Official. Official Passports are used by Government employees traveling on official business. We also make secure travel documents for other Federal agencies, including a travel booklet for the Immigration Service and another booklet for the Coast Guard.

The security of the e-Passport would be useless without securing the manufacturing process and supply chain. GPO has implemented and continues to improve the security of its supply chain. All e-Passports are manufactured under serial number control. By assigning a serial number to the chip each credential is tracked throughout the assembly process. The same serial number is used when the finished credential is personalized. Vendors are regularly audited and reviewed and requirements are continually being improved as procurements expire and are re-bid to bring the extended supply chain under even closer Government control.

Smart Cards The success and experience of our e-Passport program has enabled us to create an expanded family of e-credentials, incorporating proven e-Passport electronics, to assist Federal agencies in meeting the requirements of Homeland Security Presidential Directive 12 (HSPD-12), requiring all Federal agencies to provide employees and contractors with a Smart Card ID by the fall of 2008. These services can also be brought to bear in the compliance with the security and intelligent document standards mandated by the Intelligence Reform Act of 2004.

Based on electronics similar to those used in the e-Passport, Smart Cards grant access to Government facilities, networks, information, and other resources. Utilizing the same principle of layered security adapted for application to polycarbonate and other plastic materials, Smart Cards are composed of layers of printed and non-printed material and contain a programmable chip and antenna. An RFID (Radio Frequency Identification Device) card, a close relative of the Smart Card, contains a small, usually non-programmable chip along with an antenna. In addition to designing and manufacturing Smart Cards, GPO is in the process of procuring the capability to provide card personalization. In the personalization process, the Smart Card chip is loaded with the bearer's identity information, biometric data, and permissions.

To date, GPO has designed the security printing for two card-based identification systems. The most recent, the Trusted Traveler, SENTRI, and NEXUS Cards for the Department of Homeland Security, confirm identity and speed border crossing for regular, pre-registered, low-risk travelers between the United States, Canada, and Mexico. GPO has also designed the artwork and non-electronic security features for the new Department of Defense (DOD) Common Access Card (CAC). This is the identification card for all U.S. armed forces personnel and is currently being phased into the DOD system to provide additional visual security features and to comply with new HSPD-12 standards. This card provides both visual and electronic identification as well as physical and logical access to buildings and systems using its electronics. GPO also assisted the Social Security Administration (SSA) in designing the new security features of the Social Security Card.

When a Smart Card is brought close to or contacts a reader, the transmission of the identity information is often protected by Public Key Infrastructure (PKI) encryption, ensuring the highest level of protection for electronic information that travels over ordinary, non-secure networks. At GPO, PKI is used three ways: to protect personal information on an e-Passport or Smart Card from electronic eavesdropping; to issue certificates of authenticity for electronic documents provided through our Library Services Program; and to enable our customers to issue their own certificates of authenticity. This speeds the process by which official Government documents are submitted to the *Federal Register* and other journals of Government. The GPO has recently been designated as a Shared Services Provider for PKI, one of two Federal civilian agencies with that designation.

GPO Security and Intelligent Document Consulting and Design Services Our security and intelligent documents consulting and design services have been sought by the State Department, Department of Defense, Department of Homeland Security, FBI, Coast Guard, and the Social Security Administration. We have also made recommendations to the Real ID Standards Committee, participating through the Document Security Alliance (DSA), where our security documents expert sits on the board. We have worked closely with agencies like these to propose, develop, test, and improve comprehensive security credential solutions. The services we provide include fraud detection, threat assessment, and supply chain analysis, based on the secure supply chain that protects our e-credentials. We also help our customers identify the weak links in their supply chains and recommend methods by which new links can be forged.

GPO adds value to our consulting services by guiding policy formulation in organizations focused on security document policy. We participate as members of:

- the DSA
- the Federal Identity Credentialing Committee (FICC)
- the Inter-Agency Board for Equipment Standardization and Interoperability (IAB)
- the North American Security Products Association (NASPO)
- the ICAO

By integrating GPO expertise in security credential design, security printing, e-credentials, Smart Cards, and PKI, GPO stands ready to provide Federal e-credential expertise whenever and wherever we can help strengthen our national security.

Mr. Chairman and Members of the Subcommittee, this concludes my prepared statement, and I would be happy to answer any questions you may have.

Mr. TOWNS. Mr. Temoshok.

STATEMENT OF DAVID TEMOSHOK

Mr. TEMOSHOK. Good afternoon, Chairman Towns.

Mr. TOWNS. Do you want to pull that mic over to you? Thank you.

Mr. TEMOSHOK. Good afternoon, Chairman Towns, Congressman Bilbray and Congressman Welch. Thank you for the opportunity to participate in today's hearing on behalf of the General Services Administration.

Homeland Security Presidential Directive 12 was signed by the President in August 2004. It established the requirements for a common identification standard and credentials to be issued by Federal agencies to Federal employees and contractors to gain physical access to Federal facilities and logical access to systems and networks. The directive specified that the technical requirements for the secure credential meet four control objectives.

The credential should be, first, issued based on strong criteria for the verification of an individual's identity; second, strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; third, able to be authenticated electronically; and fourth, issued only by providers whose reliability has been established by an official Government accreditation process.

Significant strides have been made to deploy a very complex set of technologies for HSPD–12 cards and credentials in an effective and cost-efficient manner that is sustainable into the future. The National Institute of Standards and Technology [NIST], was directed by the Presidential directive to create standards and requirements for the security and the interoperability of the cards and processes required for the Government-wide implementation of HSPD–12. Accordingly, NIST issued Federal Information Processing Standard, FIPS 201, the Personal Identity Verification Standard, in February 2005. GSA established the FIPS 201 Evaluation Program in May 2006 to evaluate commercial products and services for conformance to the requirements of FIPS 201. With NIST, we have established 23 categories of products and services such as SmartCards, card readers, fingerprint scanners, card printing equipment, and the like, that require evaluation and testing for conformance to the FIPS 201 requirements.

Commercial industry has responded quickly and effectively. There are now more than 300 compliant products approved for Government-wide use for the implementation of HSPD–12.

To meet the mandates of the Presidential directive, NIST published requirements for HSPD–12 identification credentials in FIPS 201. The cards are tested and approved to meet the following requirements: They are SmartCards, incorporating at least one integrated circuit chip. The physical printing of the PIV cards provides for standard appearance and mandatory printed information. The PIV cards' integrated circuit chips possess the capability to perform data exchange interfaces in both contact and contactless modes. The PIV cards must contain the following digital credentials: A personal identification number, a cardholder unique identifier, a number, two fingerprint biometric templates, and cryptographic authentication credentials.

For security and privacy protection, all PIV data stored on the integrated circuit chip may be accessed by contact interface only following card activation through successful PIN entry. Thus, the PIV cards provide for multiple digital credentials to accomplish electronic authentication as mandated by the Presidential directive. Depending upon the level of authentication assurance required for physical or logical access, PIV card credentials like the Personal Identification Number, the cardholder unique identifier, the biometric identifiers or the cryptographic credentials may be used singly or as multiple form factors to accomplish the highest levels of authentication assurance.

To accomplish the second control objective of the Presidential directive, FIPS 201 requires both physically printed and electronic security controls for the PIV card. All PIV cards are required to contain security features that aid in reducing counterfeiting, are resistant to tampering and provide visual evidence of tampering attempts. Examples include laser etching, optically variable ink, micro-printing, holograms, holographic images, and watermarks.

PIV cards also are required to possess the capability for electronic security controls using the cards' cryptographic functions. These controls include the validation of the PIV authentication certificate, the validation of the digitally signed objects on the card and the cryptographic challenge response using the cryptographic functions. This represents the highest level of security and anticounterfeiting technologies.

Mr. TOWNS. Thank you very much for your testimony.

[The prepared statement of Mr. Temoshok follows:]

STATEMENT OF

DAVID TEMOSHOK

DIRECTOR, OFFICE OF TECHNOLOGY STRATEGY

OFFICE OF GOVERNMENTWIDE POLICY

U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,

ORGANIZATION, AND PROCUREMENT

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

OCTOBER 18, 2007

Congressman Towns, and Members of the Subcommittee, thank you for the opportunity to participate in today's hearing, my name is David Temoshok from the U.S. General Services Administration (GSA).

I am the Director of the Office of Technology Strategy's Identity Management Division in the GSA Office of Governmentwide Policy. The Office of Technology Strategy's Identity Management Division has been responsible for drafting policy standards for compliance assurance and contract turn-key solutions for identity cards for the Federal workforce as required by Homeland Security Presidential Directive #12.

Homeland Security Presidential Directive 12 (HSPD-12), signed by the President in August 2004, established the requirements for a common identification standard and credentials to be issued by Federal agencies to Federal employees and contractors to gain physical access to Federal facilities and logical access to systems and networks. The Directive specified that the technical requirements for the secure credential meet four control objectives. The credential should be

1. issued based on strong criteria for the verification of an individual's identity;
2. strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
3. able to be authenticated electronically; and,
4. issued only by providers whose reliability has been established by an official accreditation process.

Significant strides have been made to deploy a very complex set of technologies for HSPD-12 cards and credentials in an effective and cost efficient manner that is sustainable into the future. The National Institute of Standards and Technology (NIST) of the Department of Commerce was directed by the Presidential Directive to create standards and requirements for the security and interoperability of the cards and processes required for the government-wide implementation of HSPD-12. Accordingly, NIST issued Federal Information Processing Standard (FIPS) 201, The Personal Identity Verification Standard, in February 2005. NIST has issued additional technical specifications to ensure that the cards, data stored on the cards, and data interfaces are standardized across government implementations. GSA established the FIPS 201 Evaluation Program in May 2006 to evaluate commercial products and services for conformance to the normative requirements of FIPS 201. With NIST, we have established 23 categories of products and services (e.g., smart cards, card readers, fingerprint scanners, facial image capture equipment, card printing equipment, etc.) that require evaluation and testing for conformance to FIPS 201 requirements. Commercial industry has responded to the FIPS 201 requirements quickly and effectively; there now are more than 300 compliant products approved for government-wide use for the implementation of HSPD-12. We publicly post all approved products on the FIPS 201 Approved Products List at our website: www.idmanagement.gov.

To meet the mandates of the Presidential Directive, NIST published requirements for HSPD-12 identification credentials in FIPS 201. Compliant credentials are referred to as Personal Identity Verification (PIV) cards and are tested and approved to meet the following FIPS 201 requirements:

- PIV cards are "smart" cards that contain at least one integrated circuit chip for data storage and computational functions;
- Physical printing of PIV cards provide for standard appearance and mandatory printed information, which includes: color picture, name, employee, organizational affiliation, card expiration date, card serial number, and issuer identification (any other data fields are optional);
- PIV card integrated circuit chips possess the capability to perform data exchange interfaces in both contact and contactless modes;
- PIV cards must contain the following digital credentials: Personal Identification Number (PIN), cardholder unique identifier (CHUID -- a unique number assigned to the specific card, similar to a credit or debit card number), two fingerprint biometric templates, and PIV cryptographic authentication credential (asymmetric key pair and corresponding PIV authentication certificate).
- For security and privacy protection, all PIV data stored on the integrated circuit chip may be accessed by contact interface only following card activation through successful PIN entry; the only PIV data permitted for contactless interface is the cardholder unique identifier (CHUID).

Thus, PIV cards provide multiple digital credentials to accomplish the electronic authentication mandated by the third HSPD-12 control objective. NIST published Special Publication 800-63, Recommendations for Electronic Authentication to provide identity authentication requirements for the four authentication assurance levels established by the Office of Management and Budget in Policy Memo M-04-04. Depending on the level of authentication assurance required for the physical or logical access controls, PIV card credentials (PIN, CHUID, biometric templates, cryptographic credentials) may by used singly or as multiple form factors to accomplish the highest levels of authentication assurance under NIST Special Publication 800-63.

To accomplish the second control objective of the Presidential Directive, FIPS 201 requires both physically printed and electronic security controls for the PIV card. All PIV cards are required to contain security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts. Examples of such physical printing controls are: laser etching and engraving, optically variable ink, micro printing, holograms, holographic images, and watermarks. PIV cards are also required to possess the capability of electronic security controls using the cards' cryptographic functions. These controls include:

- Validation of the PIV authentication certificate;
- Validation of the digitally signed objects on the PIV card (i.e., CHUID, biometric template);

- Cryptographic challenge-response using the PIV authenticate key to perform cryptographic functions.

These cryptographic security functions are extremely sophisticated and make the PIV digital credentials virtually impossible to counterfeit. GSA tests the commercial and agency-specific PIV cards to ensure that these security functions are uniformly implemented.

GSA also spearheaded the development of standard government interfaces that will be needed to ensure that the Agency systems can exchange data and work together over the long term. This work defined a common system architecture for components and defined interface specifications for the exchange of data across HSPD-12 system components.

The GSA Managed Service Offering (MSO) was established in the fall of 2006 to provide compliant credential and identity services to Federal agencies meeting the requirements of HSPD-12 and the Federal Information Processing Standard (FIPS) 201.

GSA pursued the managed services strategy to save money but also to improve service quality, and decrease implementation risk. Explicit benefits include:

- Reduced setup cost and risk from the use of a common solution with strong configuration management to ensure that all mandatory requirements are met now and in the future;
- Improved internal controls and accountability for role assignments;
- Improved economies of scale associated with sharing a common hardware and software environment; and
- Increased transparency of services through Service Level Agreements, performance measures, and predictable upgrades.

The MSO is currently serving 67 agencies and commissions with the responsibility to provision and manage over 800,000 electronic identity accounts. This is approximately 50 percent of the civilian Federal population. The MSO allows agencies to offload the difficulty of meeting the FIPS credentialing standards and managing the electronic identity while agencies have continued accountability for providing accurate employee identity data and managing the status of their employees. GSA succeeded in aggregating the needs of multiple agencies to produce volume and cost efficiencies in delivery of credentials as well as providing enrollment infrastructure across the US to efficiently serve both the federal employee and contractor populations who fall under FIPS rules. The service provides a sophisticated identity infrastructure needed to meet FIPS requirements as well as logistics support such as enrollment stations, labor, training, and help desk support needed for high availability, both in normal and emergency situations. Information on the GSA MSO service is available at www.FedIDCard.gov. The GSA Team continues to work closely with all customers to ensure compliance with HSPD-12 requirements.

GSA offers the approved products and services for HSPD-12 implementation on GSA Multi-Award Schedule 70 for government-wide acquisition. GSA has created Special Item Numbers 132-61 and 132-62 for HSPD-12 approved products and services. An amendment to the Federal Acquisition Regulations requires that only approved products be incorporated in agency implementations. The approved products and services on Information Technology Schedule 70 are also available to state and local governments for cooperative purchasing.

In summary, HSPD-12 has had significant participation from industry and Federal agencies. Significant progress has been made in a relatively short amount of time without compromising on the goals of the program and with serious consideration on how to achieve cost-effective implementation. I am happy to take any questions you may have.

Mr. TOWNS. Ms. Rutledge.

STATEMENT OF BONNIE RUTLEDGE

Ms. RUTLEDGE. Thank you. Good afternoon, Chairman Towns and other distinguished members of the committee.

My name is Bonnie Rutledge, and I am the Commissioner of the Department of Motor Vehicles for the State of Vermont. I have been with the Department for 37 years. I am also a former chair of the board for the American Association of Motor Vehicle Administrators, and I wish to thank you for the honor to be here today and to give testimony on what Vermont is doing to enhance our driver's license for uses other than a document indicating the individual has been licensed to drive.

Even though the original intent of the driver's license was just to license an individual to operate a motor vehicle, over the years, it has become the most widely accepted form of identification. While credentials can be made as tamperproof as possible, if the issuance process for the major identification cards is not made more secure, the preponderance of identity document fraud will continue.

Most fraud is committed by criminals enrolling in a system under a false identity. Before an agency can issue a secure credential, sound technology and policies, procedures and business systems must be in place. The privilege of retaining ones driver's license has been used to assure taxes are paid, that child support obligations are met, to provide the opportunity for one to register to vote, and other similar uses. With these added responsibilities, it has become most important that making sure the individual obtaining that license is who they say they are and then, once the document is issued, that it is secure.

Long before the tragic events of 9/11, Vermont began taking steps to verify identity and to produce a secure document. The most recent responsibility our State has accepted is to issue an Enhanced Driver's License that will allow Vermont citizens who qualify to use the driver's license as an approved alternative document for reentry into the United States at land and sea borders between the United States, Canada, Mexico, Bermuda, and the Caribbean. This agreement between the State of Vermont and the Department of Homeland Security was to preserve travel, trade and cultural ties, in particular between Vermont and Quebec, and to assist with increased security at the border while allowing less time for legitimate citizens to cross the border.

Currently, Vermont driver's licenses are produced over the counter, and the customer leaves with the document. The Enhanced Driver's License will be produced in a central issue environment. The customer will be given a temporary license while the necessary identity and immigration verification checks are completed, and the enhanced license will be mailed within a week to 10 days. Current Vermont cards are compliant with the material and design standards of the American Association of Motor Vehicle Administrators' card security framework, a national driver's license card security standard. Vermont uses watermarking, micro-printing, fine-line background, Tri-Color Polasecure with U.V.—which incorporates three-color graphic designs printed on the inside of the

laminate and ultraviolet sensitive inks—redundant data, overlapping graphics, ghost image, bar code, and magnetic stripe along with various covert and overt features shared only with law enforcement. The ultra-high frequency, passive vicinity RFID tag and machine readable zone, as well as the designation of the Enhanced Driver's License, will be added to the Enhanced Driver's License.

Ultra-high frequencies typically offer better range and can transfer data faster than low and high frequencies. Passive RFID tags do not have a power source. They draw power from the RFID reader to energize the microchip circuits. The antenna enables the tag to transmit the information on the chip to a reader. The reader converts the radio waves reflected back from the RFID tag into digital information that can be passed on to computers to make use of it.

The vicinity RFID tag will be read by the border crossing agent as a licensee approaches the border checkpoint. This will allow the process of verification to begin prior to the individuals' actually presenting themselves to the agent. The RFID chip will not retain any information other than a unique identifying number that will access the Vermont DMV data base to retrieve the information contained on the front of the Enhanced Driver's License identification card. Data encryption, secure networks and firewalls will protect the transmission of the information. For added security, the DMV will provide a security sleeve to protect the RFID tag from being read when the cardholder is not at a border crossing station. The DMV will fully disclose the nature of the RFID, its purpose, content and security to all Enhanced Driver's License identification card applicants and interested parties. The MRZ will contain the information that is on face of the license and will be used at all crossings that are not RFID-enabled.

With the impending requirement for a passport for all border crossings, Vermont felt it was timely to enter into this agreement. There have also been discussions with Homeland Security regarding the time of the passport requirement and the implementation date for our new licenses as well as for the use of the Enhanced Driver's License for domestic air travel in the future. It is also Vermont's desire that the Enhanced Driver's License would complement the REAL ID requirements and are awaiting the final rule to be published.

I've submitted a more detailed document in writing regarding Vermont's business processes for issuing licenses and the technology employed.

Once again, I thank you for the opportunity to speak on this very important topic.

[The prepared statement of Ms. Rutledge follows:]

18 October 2007

The Honorable Edolphus Towns
Chairman
Subcommittee on Government Management,
Organization, and Procurement
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515-6143

Dear Congressman Towns:

I am honored to be asked to submit testimony on the subject of "Technology for Secure Identity Documents". Vermont is continually employing technologies that will ensure our documents are secure. Since the driver's license is the mostly widely accepted form of identification it is necessary that the process for issuing and the document given to our citizens is as secure as possible.

Attached are Vermont's written comments and I look forward to giving an oral summary at the hearing.

Very truly yours,

Bonnie L. Rutledge
Commissioner

:blr
Enc. 1

State of Vermont License Security

Vermont Department of Motor Vehicles current business process for the issuance of a standard license

Over the years a Drivers License has become the most widely accepted form of identification. It is the heart of our identification infrastructure and is taking a central role in the efforts to protect our homeland. While credentials can be made as "tamper proof" as possible, if the issuance process is not secure, the preponderance of identity document fraud will continue. Most fraud is committed by criminals enrolling in a system under a false identity. The State of Vermont has sound technology, policies and business systems in place to ensure the security of our license.

It is our goal to ensure that every individual is limited to one license document, and one driver control record

- Employees issuing a Vermont Driver License or Identification Card (DL/ID) are subject to criminal background checks.
- One employee completes the entire process from application to processing of the DL/ID, eliminating the possibility of "customer swap" whereby customers attempt to switch during the process.
- All materials used for license production are inventoried and stored in secure locations
- Various electronic checks are performed to validate Social Security Numbers, and to ensure the customer does not have another license or any outstanding suspensions.
- Standards are in place for computer security and unauthorized access. Audit trails will be maintained to support security and access functions. The State's Department of Information and Innovation (DII) and Agency of Transportation (AOT) both require personal user log-ins and passwords. The digital capture workstations (DCW) cannot be accessed without proper authorization and proper security dongle. All access creates an audit trail.
- Our employees all receive fraudulent document recognition training.
- We have adopted privacy principles and practices to ensure the protection and confidentiality of all personal information contained in the agency's records

Current workflow;

1) Greeter station; customers are checked in and we verify that they have proper forms and identification
2) Verification process to ensure that new applicants do not hold a driver's license from another jurisdiction
3) Applicant identity verification station; paperwork is processed, identity is verified and fees are collected
4) Vision, knowledge, and skills testing are administered if applicable
5) Image/demographic information capture station, customers photo and signature are digitally captured, license is printed and handed to customer.

State of Vermont License Security

Vermont Department of Motor Vehicles proposed business process for the issuance of EDL/ID

The Enhanced Driver License/ Identification (EDL/ID) workflow includes the above, but adds the scanning of identification documents, adds a station to print a temporary EDL/ID, and adds a station where a short interview is conducted to further qualify applicants.

The EDL/ID will add a number of additional enhancements to include;

The State of Vermont will require full accountability for all materials, including usage and destruction. Standards will be in place for the overall security of materials used in production, and for the loss or theft of blank documents/materials. All blank document materials are to be held in a separate secure repository with controlled access. Physical inventory of all production materials is to be conducted every week. The State of Vermont must be able to, at any time during this process, have the ability to call selected contractors facility and delay printing or pull an individual driver license out of production because an investigator or police officer has identified potential duplicate, fraud, legal presence issue, or other potential problem during the document authentication and data verification process.

Enhanced Driver license / ID cards will include document security features designed to deter forgery and counterfeiting and promote confidence in the card format.

Vermont cards are compliant with material and design standards of the American Association of Motor Vehicle Administrator's (AAMVA) card security framework, a national driver license card security standard. Vermont uses watermarking, micro-printing, fine line background, Tri-Color Polasecure with UV which incorporates three-color graphic designs printed on the inside of the laminate and ultraviolet sensitive inks, redundant data, overlapping graphics, ghost image, bar code and magnetic stripe.[1]

The face of the card will contain name, date of birth, gender, full facial photograph, address, signature, issuance/expiration date and citizenship.

Each document will contain, at the minimum, the issue date, the citizens date of birth, gender, address, signature, Vermont license number and a full color full facial photograph. A Gen 2 vicinity Radio Frequency Identification (RFID) chip will be imbedded in the enhanced DL/ID card in compliance with DHS security standards. Citizenship status will be depicted on the enhanced driver license. The back of the DL/ID will also have a machine readable zone (MRZ) which will facilitate border crossing at locations not RFID capable. The EDL will be clearly distinguishable from a standard Vermont DL.

Issuance Procedures for the enhanced DL/ID will demonstrate an applicant's eligibility.

DMV licensing staff will determine eligibility by authenticating the documents submitted and conducting investigative applicant interviews to determine identity and citizenship. One acceptable document is a valid U.S. Passport. Other acceptable documents include a certified state birth certificate, Certificate of Naturalization, or Certificate of Citizenship; an expired U.S. Passport, or a Department of State Consular Report of Birth Abroad.

State of Vermont License Security

Address verification will be utilized to verify the address with the U.S. Postal Service and confirm the applicant's address is valid. Social Security electronic verification will be utilized to verify every number with the Social Security Administration. Signature comparisons will be conducted on every applicant when possible.

All applicants for EDL/ID will be subject to an interview. The interview is designed to further establish a link between the applicant and the source documents. Staff will receive additional investigative interview training to look for behaviors that may suggest an imposter or intent to commit fraud. This additional step, coupled with new web-based technology and authentication of source and identity documents by trained staff significantly increases the reliability of the application and approval process.

Technology Requirements

Vermont's EDL/ID will use facilitative technology and share biographic information (including photo) with DHS.

DMV will employ facilitative technology in the enhanced DL/ID. The enhanced card will incorporate both the vicinity RFID chip and MRZ. In addition, border crossing personnel will have electronic connectivity to DMV.

The vicinity RFID or MRZ technology will assist border crossing personnel by providing a unique identifier. The unique identifier will be used to provide DHS with digital photos, biographic information and validity information. RFID technology will provide information prior to the vehicle arriving at the inspection booth. Real-time access will be used to validate the enhanced DL/ID with DMV's database.

---

[1] **Watermarking** – details limited to law enforcement

Micro-printing - Commonly found on national currencies, micro-printing complicates any attempt at photocopying due to the resolution required to recreate the feature. It can be read with an eight (8x) power magnifier.

Fine line background - a pattern of fine lines, similar to those found on national currencies

Tri-Color Polasecure with UV - three optically variable inks printed on the card's inner laminate. Optically variable inks appear and disappear with the variation of the viewing angle and make attempted alterations readily apparent.

Redundant data – Certain data elements are repeated, some obvious and some contained within barcodes

Overlapping graphics – placing information over the picture to complicate any attempt to change the picture. State seal and commissioners signature overlap the photo.

Ghost image – printing the picture in more than one location

Bar code – 2D bar code encoded with AAMVA minimum standards

Magnetic stripe – magnetic stripe contains Name, DOB, Height, Weight

Mr. TOWNS. All right. Thank you very much.

Let me thank all of you for your testimony.

I'll, I guess, begin by first saying: Do you feel that costs might be something that would permit us from moving forward in a very aggressive fashion?

We'll start with you, Ms. Kraninger.

Ms. KRANINGER. Certainly.

Cost is certainly a factor as we look at the way in which we move forward with these programs, particularly from a number of vantage points. First, you start with the business case by saying, "What is the level of security that is required? What is the risk that is posed? Then what exactly will counter that risk in terms of what is available today and for what cost?"

If you take a sector like the Transportation Worker Identification Card—which I also do have an example here for you to see and some other exemplars of fraudulent documents after the hearing if there's interest—the TWIC card, it's being issued based on a legislative mandate to secure access to secure areas of ports. Given that critical need and the need to do a full background check, an immigration status check, a terrorist watch list check, and to collect ten fingerprints from and a photograph of each of the maritime workers who will get a TWIC card, that translated into the need for also a highly secure document that could be read in a decentralized way so that each facility, when they employ access control, can use this biometric card to actually use in their access control system.

So this is a highly secure document, and it is a very—it's a shared process that follows the FIPS 201 standard that is in place, underlying HSPD–12, for Federal identity documents as well. So that's a very high level of security, a very high-risk area and something that is pertinent to a particular industry.

When you look at the requirements that we will levy on driver's licenses and setting minimum standards under the REAL ID Act, there is a consideration there again about the risk, the state of the industry and what makes sense from a business standpoint, and we certainly took into consideration all of the comments that we received from the Departments of Motor Vehicles, including the DMV of Vermont when they said what was possible and what makes sense from a cost standpoint as well. So that is certainly a factor as we look at these things, as well as privacy considerations, that are all part of the decisionmaking process.

Mr. TOWNS. All right. Thank you very much.

Ms. Rutledge, first of all, let me salute you. I think you're taking the right step by combining the driver's licenses with the border crossing, but as I understand it, even this new driver's license will not necessarily comply with the REAL ID law; is that true?

Ms. RUTLEDGE. Well, I'm not sure, sir, because the final rules have not been published yet.

What we have in place right now complies with the act, itself, and has been in compliance, but as far as the rules go, I don't know as yet. In discussions and in looking at the rules over the years and the proposed rules, we would not be in compliance. For one thing, our Enhanced Driver's License will be a voluntary program for those individuals who would qualify and who would want to have one. Under the REAL ID Act, everybody would be required to go

through the reenrollment process, and for every State, that's where the huge cost comes in, not only to the Departments but also to the individuals, because they would be required to present themselves, once again, along with their identity documents to prove who they are—every driver and everyone getting an identity card.

Mr. TOWNS. So you are hoping that we just won't get in your way.

Ms. RUTLEDGE. That is our hope.

Mr. TOWNS. That's what I thought.

Mr. WELCH. Vermonters, Mr. Chairman.

Mr. TOWNS. How about that? Right.

Now, whether it is a border crossing card or an Enhanced Driver's License, there has been a lot of concern that data from RFID cards can be read by as much as 30 feet away.

If citizens are carrying this card around with them, could their movements be tracked?

Mr. BILBRAY. Do you mean like a cell phone?

Mr. TOWNS. Yes, like a cell phone.

Ms. KRANINGER. Mr. Chairman, I'm happy to take that question, and Bonnie can add with respect to Vermont's perspective on this as we've talked about it.

I think, to Mr. Bilbray's point, there are certainly many ways that individuals can be tracked at that distance—by sight, by the driver's vehicle license plate and certainly by cell phones. So, when it comes to the risk/reward decision, each individual, as Bonnie noted, will be making this decision based on their own read of the situation.

For our part in examining this technology in the business case, we determined that the best way to address this particular concern is by, one, putting it in perspective of other risks, but two, we are going to be giving out the document with a sleeve that is a protective sleeve, quite frankly. It blocks the transmission of the signal, and so the individual will have notice and understand the way the technology works and have the sleeve that they can keep their driver's license in if they're concerned about that particular issue and, thereby, can counter that.

Mr. TOWNS. Anyway, let me yield to—I'm trying to figure would it be possible for—anyway, let me yield to my ranking member, because I have the clock on me there.

Mr. BILBRAY. Mr. Chairman, let me just make you feel better. As somebody who served on the subcommittee that did the telecommunications bill back in the 1990's, it was a Federal mandate that your phone has a GPS chip in it now that can be tracked even when it's off. So if that makes you feel any better——

Mr. TOWNS. Right. Right.

Mr. BILBRAY. The other issue would be, obviously, those of us who have credit cards and that we're able to be tracked on that, so there are a lot of these convenience items that not only are part of the private sector, but the Federal Government mandated the phone tracking capabilities to be in our cell phones.

So, Ms. Kraninger, the question is this. While we're talking about the use of technology and how it works or whatever, if there were any State—and I need to apologize to the chairman because we want to be bipartisan—but I am going to point out that, though

our Governor, who is an immigrant, has fought strongly for securing the identification systems in California, I was very surprised to see the Governor of New York announce that he was going to eliminate the requirement for Social Security cards and was actually going to issue driver's licenses based on, purely, something like the passports that would have been one of those great black market items in there.

Could you articulate at all if we've got a problem or could have a major problem with States' taking that kind of a step toward accepting the base documents for their identifications and how that affects the whole system?

Ms. KRANINGER. Certainly, we are concerned as we look across the States and recognize that many of them, including New York, have taken extensive steps in the past few years to further secure their driver's license issuance process: what they base the issuance on, how individuals are demonstrating identity and residency and legal presence, as well as the security features in the documents, themselves.

Of course, with respect to this particular issue, the States are responsible primarily for ensuring driver safety, and while DHS has been intensely focused on secure identification and the security of the driver's licenses, we want to, first and foremost, focus on that identity portion. We want to make sure that front-line officers and all law enforcement can have confidence in the documents that are presented to them and that those documents are secure.

When REAL ID takes effect, of course, we will not accept non REAL IDs, those documents that do not actually demonstrate legal presence for Federal purposes. So that includes boarding domestic flights and entering Federal facilities. So anything that conflicts with our efforts to increase secure identification is of great concern.

Mr. BILBRAY. You know, if there were ever a State that has been impacted by this more than anybody else that I know of in our world it is the State of New York. It is the great tragedy there. Wasn't this one of the real strong recommendations of the 9/11 Commission?

Ms. KRANINGER. It definitely was, yes, the implementation of REAL ID as well as the security of travel documents.

Mr. BILBRAY. Ms. Rutledge, the real leader in this that really is the unsung hero in so much of this stuff is, actually, your national organization, the AAMVA.

Ms. RUTLEDGE. Yes.

Mr. BILBRAY. I don't think the public even knows that, as far back as 1996, you guys were saying we need to have Federal leadership here working with the States and doing something about this, because the potential is out there, and it was almost, you know, such a perception over the horizon of what could happen on 9/11, and you guys did it in 1996, and I think a lot of people were shocked as to how much your national organization was able to get together the month after 9/11 and then tool it up and have the recommendations out there for the Federal Government, and I have to tell you, it was really cutting edge. I think anybody working day-to-day could see that this problem was eventually going to happen, and it's sad that we didn't listen to you guys in 1996, 1997, 1998,

and it took 9/11 to finally say: "Maybe we ought to get involved with this stuff."

I am interested in your personal—because, I think, coming from local government—I mean, I served as a mayor. I was the chairman of San Diego County, a small, intimate group of 3 million people in one county, but your State, to me, is really exciting, because you've got the size to really prove it through practical application.

I just cannot perceive that you cannot be working with the Feds, and everything that I hear you're doing is going to fulfill REAL ID so that Americans don't have to carry their passports in their back pockets; their driver's licenses will be viable, but that's based on the security of that document, isn't it?

Ms. RUTLEDGE. And the process of issuing that document, sir, yes.

Mr. BILBRAY. Now, the question there as you were talking—and if I may just followup on this, Mr. Chairman.

You're still going to have those driver's licenses that are under that. Even if everyone doesn't opt into it, your citizens will have the opportunity to opt into this ID system, and those cards will be acceptable. As far as I know, Homeland Security said that will qualify. Right now, they're saying a passport or another recognized Federal, you know, document, and that will qualify. So your citizens who don't qualify for it, they won't be able to get on an airplane, open a bank account or cross the border with the old driver's licenses, but you will then have the opportunity in your State for your citizens to voluntarily get into this system so that they have the ability to participate in the program.

Ms. RUTLEDGE. For the Enhanced Driver's License, yes.

Mr. BILBRAY. OK. Madam Chair, I just think that there was a—Mr. Chairman, I would just say that I think this is a good example of where we can learn by doing, and it's really a great State to do it on because you're a manageable size. It's not like 35 million people in California, which is going to be some heavy lifting.

Thank you very much. I yield back, Mr. Chairman.

Mr. TOWNS. Thank you very much.

I agree with you, because her State is the size of my congressional district.

I yield to Congressman Welch.

Mr. WELCH. And her State is the size of my congressional—her congressional district is the size of my State. I am going to take the opportunity to talk to Ms. Rutledge.

We are doing an experimental program. You've worked with the Department of Homeland Security, and Mr. Chertoff came up and met with our Governor Douglas, a Republican and friend, and you have been given some permission, I guess, to do something on an experimental basis; is that right?

Ms. RUTLEDGE. Correct.

Mr. WELCH. I've two questions.

One, maybe describe that very briefly; but two, there's another State that's doing that as well, and I think we're doing the same as they, and I'm wondering whether—this is really my second question: Do you think there might be some advantage to giving us in Vermont some flexibility outside of—to do it our way? Obviously,

it's in coordination with the Department, because the ultimate—the goal here is to have security but, also, ease of travel.

So can you comment on those two questions?

Ms. RUTLEDGE. Absolutely.

In my many years of working at Motor Vehicles, especially in a small State, I've figured out it's best for Vermont to either be first or last because, if you are first, you have the ability to help craft how the process is going to look, and Homeland Security has been working very closely with us to make sure whatever we do fits for us. We are not a California or a New York or others, but we do have a lot of things in place that, perhaps, those large States don't do.

We have a very good working relationship with Immigration. On a one-to-one basis, we can call them to do a verification as opposed to having to do it electronically if we have to. So, because of our size, we do have a lot of pluses, and yes, we are doing it first so that we can help craft how it's going to look.

Mr. WELCH. Well, would you like to have any more flexibility? I mean how is it that we're doing it now? It's the same as what? Is it Washington?

Ms. RUTLEDGE. The State of Washington, yes.

Mr. WELCH. Right.

Ms. RUTLEDGE. We're pretty much following them. Our business plan may be a little bit different than theirs is, but there aren't a lot of differences.

Mr. WELCH. OK. Thank you.

I yield back the balance of my time. Thank you.

Mr. TOWNS. Thank you very, very, very, very, very, very much. You know, I still want to go back to this.

Even if we see and feel that this is what needs to be done and we sort all of these things out, then we look at the costs, and we begin to back away because of costs.

Mr. Temoshok, let me ask you: How do you feel about the general support system out there for—you know, once we know what we want to do and we look and we find out that it's going to cost a whole lot, what are we going to do then?

Mr. TEMOSHOK. Well, without question, cost is a factor in implementation. In the Federal Government for HSPD–12, because this was a Presidential directive, agencies are directed to implement these security provisions.

One of the strategies for implementing HSPD–12 across government was to be able to facilitate how agencies implement the Presidential directive. Having every agency develop the infrastructure to issue SmartCards, to produce SmartCards, to manage that security process certainly would not be the most efficient or the most timeworthy means of implementing the directive.

With the Office of Management and Budget, we designated agencies to offer shared services, to provide the infrastructure to comply with HSPD–12, to provide compliant Security Services' cards, the management of identities on behalf of Government agencies—the Department of Defense, the four branches of the military, the Department of State, for the agencies that are housed with them internationally, and the GSA for the rest of the civilian Government.

Currently, we provide services to 67 agencies. It simply would not be economically feasible for those agencies to implement under this timeframe without using the GSA shared services. By aggregating requirements within the shared service offerings, we are able to consolidate and reduce the costs. It's still a factor, but we've significantly reduced the costs for complying with the Presidential directive for the agencies that are using the shared services. Presently, more than 65 agencies use GSA's shared service. About a dozen agencies are implementing HSPD–12 systems on their own.

Mr. TOWNS. Are you hearing people saying, "Are the benefits worth the costs?" That's my concern.

Mr. TEMOSHOK. Every agency in the government has not just one badging process and badging system but, potentially, many different badging systems. I would contend that all of the different, various badging programs currently cost much more than it will cost to comply with a single standard secure process under the Presidential directive.

Does it warrant the cost? Do the benefits warrant the cost? The security of our facilities and the security—the secure access to our systems and networks is worth that cost.

Mr. TOWNS. I yield to my ranking member for any further questions.

Mr. BILBRAY. Let me say I appreciate that. I think that as this comes up, the Federal Government does a lot of things that's not mandated in our constitutional obligations. We do a lot of stuff. One of those things is the interstate commerce clause and the national security clause. This falls right into that category, be it giving citizens the ability to cross international borders or to getting on airplanes or to opening bank accounts under the commerce clause or to stopping identity theft, and I mean this falls into this.

I guess, Mr. Chairman, when we talk about costs, what was the cost of 9/11? The fact is, remember, the 9/11 terrorists were given driver's licenses by Virginia, so they did not have to show their Saudi Arabian passports, which then could have triggered a whole new—you know, a whole defensive mechanism.

What is the cost of stolen identities here in the United States? It is huge, especially when you consider the fact of how many unlawfully present people have to falsify and steal IDs to be able to get employment services and a lot of other things. What does that cost in the long run?

I think that, when we get into this cost of, you know, how important security is, we could go over and ask the Finance Committee about what was the cost for us upgrading our currency in this country. It was huge, but it's worth every cent.

So I just have to say the one thing, though, is that I look at certain aspects of it like the Ag Department where they have 170,000 employees but have only issued seven cards. We really are needing to lead it stronger than we have in the past, and that's a concern we have over there.

Ms. Rutledge, I thought your State had some real problems with ID or were there some political repercussions of it in your State?

Ms. RUTLEDGE. No, not that I'm aware of.

Mr. BILBRAY. OK. I appreciate that. I know there are some States that are kind of goosey about it, but the more that I'm see-

ing States look at, you know, the new initiatives, you know, they're sort of realizing that REAL ID is a vehicle that we could work over on them.

Mr. TOWNS. It was probably New York.

Mr. BILBRAY. Yeah, it was probably New York.

Ms. RUTLEDGE. Well, actually, since the announcement of the Enhanced Driver's License, we've been inundated with calls from people who want to know how soon they can get it.

Mr. BILBRAY. Well, let me just tell you, as somebody who spends a lot of time crossing a lot of different borders and international boundaries, too, that the convenience is one thing, and—I'll just say this to General Services that, I guess, it was the new visit system. Anyone who says that they're scared of the use of technology should talk to immigrants who are going through the visit system now. It is so refreshing to hear them. Immigrants or visitors who are coming back, they stick their passport in; they put their hand in, and they're told. And, it's none of these 50 questions and getting a cross-examination and feeling like a criminal. The immigrants and the visitors who use this technology just praise it right and left, and I think that it's one of those things that we ought to talk to our visitors about and see how the system is working.

I will basically open up to one question, and that is: When can we see the Federal Government leading with this? What is our timeline? When will we get down there? Because basically, what I'm seeing is the States are going to lead, and maybe that's not bad as a local government guy, but when are we going to catch up? When are we going to have more than seven cards out there?

Mr. TEMOSHOK. The USDA is one of GSA's customers in the shared service that I described. We are in the process within GSA to implement enrollment stations across the country wherever we have customers, and since we will need to enroll over, currently, 800,000 employees and contractors into the HSPD–12 program, we will need enrollment stations all over the country. We are focusing in Washington, DC, first. Our target by October 2008 is to enroll all of our customers into the program and to issue cards to them.

Mr. BILBRAY. OK. Well, just to let you—I mean, I don't want to beat up on one. I mean, in Human Health Services, you've got over 100,000 employees there, and you've got four cards issued. For the archivists, they have 3,000 employees, and we have three cards issued. So I mean there is—we're here to sort of encourage you along. That's why they call us "oversight."

Thank you very much, Mr. Chairman.

Mr. TOWNS. Thank you very much.

I'm going to use the balance of your time. You had a little time left. I'm going to use it.

Let me ask you, Mr. Brink. We saw a lot of problems this summer with passports, I mean huge problems, and the State Department just couldn't handle the increase in the applications caused by the new requirements, I mean, we received phone calls all over the place, and there was a backlog of several months. I'm worried about whether agencies are prepared to handle the logistics of issuing new ID cards to millions of people.

What are the plans to handle big increases in volume or for HSPD–12 border crossing cards or even for State-issuing driver's licenses?

Mr. BRINK. Well, of course, GPO is the manufacturer of the card, and it's not directly involved in the issuing, but I think that points out both in the cost area and also in the issuing area that's the real key to the success of these programs. It's the adjudication of applications. It's the issuing logistics. We were able to keep up by the skin of our teeth, but we were able to keep up with the citizen demand with the manufacturer, but the backlog grew within that bow wave of citizen applications to get the new passports, and that's where the backup was, and that's clearly where we need to focus if we're going to keep up, is to provide the right sort of resources to that end of the whole production and issuance chain.

Mr. BILBRAY. Mr. Chairman, can I——

Mr. TOWNS. Yes. Sure, I yield.

Mr. BILBRAY. Let me just followup on that.

It seems that the bubble has been passed, though, and that the learning curve has picked up where—I think we agree that we're not getting the calls now, that it looks like you got up to steam. Maybe there was a learning curve there. Can we build on that learning process?

On the flip side, that's one reason why I feel strongly about the States. If we can get the States to do the administration, the efficiency factor will be, as long as they can, you know, fulfill the minimum standards—we can really move. We can have the best of both worlds.

Mr. BRINK. I'd also like to compliment our customer, the Department of State. As you probably know, they brought 450 counselors/officers back from overseas and hired 400 more people to deal with that bow wave, and as we were working 7 days a week, they were working 7 days a week to get through that backlog.

Mr. BILBRAY. Well, good. If that's what it takes to serve the public, that's what we do.

Mr. TOWNS. Let me raise one other issue very quickly before we let you go.

One of the problems here is that there are so many different types of ID out there. They look different, and they use different technology. It's just not realistic to expect a bank teller or an airport screener or an employer to be familiar with all of them.

Now, without creating a national ID, why can't we settle on one technology of a visual format to be a nationwide standard for ID documents issued by different Federal and State agencies? Because all of these different IDs out there—I mean, it's just going to continue to add confusion.

I indicated to you that I was having trouble getting on an airplane in Orlando with my congressional ID. You know, fortunately, here in Washington, that's the thing that gets you on the plane, you know, but in Orlando, they have never seen that, and of course, they were not about to let me go through that line with that funny looking ID.

Mr. BILBRAY. In fact, Mr. Chairman, that was the intention of the REAL ID with the State IDs, but you're right. What about the

Feds? Are we going to do our fair share with the same thing, with a common format?

Mr. TOWNS. What do we do?

Mr. BRINK. That's probably yours because, clearly, HSPD–12 is one of the attempts.

Mr. TEMOSHOK. I'll start because, for HSPD–12 and the Personal Identity Verification cards, there is a standard format in the physical topography of the card—what they will look like and what the printed information will contain as well as the information that needs to be contained and personalized on the integrated circuit chip—but the HSPD–12 standards specifically apply to the Federal Government. As a standard, it can be adopted by other Federal programs or programs outside of the Federal Government in order to conform to that established standard.

Mr. TOWNS. Do you have any idea as to what we might do here in Congress to be able to move in that direction? Because I'm afraid that more IDs are going to be created, which leads to more confusion.

Do you have any suggestions for us here in the Congress that we might do to be able to assist?

Mr. BILBRAY. Let's say it a little differently.

Are you guys willing to live up to the standard that we set for the States?

Mr. TOWNS. That's a better question.

Mr. BILBRAY. Well, it's basically what you're asking.

Mr. TOWNS. I like that. I like that. I think that's putting it very succinctly.

Mr. BILBRAY. Are you guys ready to live up to the REAL ID standards?

Mr. TEMOSHOK. I'll address what we do for HSPD–12.

Now, HSPD–12, the Presidential directive, was explicit in directing the Department of Commerce and the National Institute of Standards and Technology to develop the standards for the Federal Government's identity management, badging and credentialing program, and they've met that directive and have published those, as I indicated, as the Federal Information Processing Standard [FIPS], 201.

Now, as we look at that and as we gear up all of the badging programs in the Federal Government and the readers who read those cards to meet those standards, it takes a significant effort, not just by the—and cost—not just to the Federal Government but to industry, and so industry has tailored their production and their products to those standards, which becomes very important, I think, both from our perspective in implementing from the Federal Government but potentially, also, from your standpoint in looking across—in looking beyond the Federal Government.

Because of the cost of those high security devices, the cards as well as the readers are being driven down by conformance to a standard in the Federal Government.

Mr. TOWNS. Let me thank all of you for your testimony.

Mr. BILBRAY. I wanted to say that we've had a good discussion here on certain aspects, and I think that the standards are one of those things.

One of the things that the chairman's concerned about, and a lot of people are concerned about, is a national ID card becoming a mandated document. And, I think the chairman will remember, one of the big reasons why REAL ID was passed was that there was a recognition in Congress that you have two choices: Either a national ID card and identification or a national minimum standard that is administered by the States and the Federal Government separately and that the national minimum standard was a much better option than a single Federal document in the past.

And I think that those of us that want to avoid the national ID card recognized that this was a great alternative as an American way of doing it. We just have everybody do it, but they do it up to a minimum standard.

The one thing that I'd ask you, Ms. Rutledge, the one Federal document used in America has not changed since the 1930's. Social security card.

Will our Federal card—or does it qualify under REAL ID? Social security card as we know it.

Ms. RUTLEDGE. That is one of the things that we use for a form of identification.

Mr. BILBRAY. But it doesn't fulfill the mandate. Our employment identification has not fulfilled the mandate that we put on you guys for the driver's license.

Ms. RUTLEDGE. Right.

Mr. BILBRAY. Is it within the executive branch's authority—do you have the power, if you wanted to upgrade that document, which is really one of the base documents, the breeder documents? Is there any discussion about the ability of the executive branch to take the initiative and upgrade that documentation?

Ms. KRANINGER. Congressman, there definitely are discussions to that end, and certainly we had that discussion particularly during the immigration reform debate. I can't speak to what Social Security Administration's authorities are with respect to upgrading the card notwithstanding some congressional action, but certainly we have looked at that and talked about it.

I think the one thing that is of note, at least with respect to Real ID, is that verification of at least that document as it is presented, and recognizing that it can't stand alone as something that could be the basis of identity depending on the privilege that is being applied for with respect to a driver's license. It certainly is not the case that is the only document that an individual would show.

Mr. BILBRAY. I want to thank you for the hearing.

I do not know of a State in the Union or a county or a city that still uses a piece of paper with a name and a number on it as an identification document. I mean, they have all upgraded except for the Federal Government, and where we have asked you to sort of get your act together, I think we are at a point where we need to sort of go back, and physician heal thyself, and do the right thing and lead by example. And, one of the things we need to talk about is, as far as I know, that there is no law out there stopping the administration from upgrading all of its identification up to a minimum standard, not picking and choosing.

So I yield back.

Mr. TOWNS. Thank you very much.

Let me thank you for your testimony, of course, and you can see and hear our concerns, and we are going to continue to look at this and to see in terms of what we might be able to do to assist.

We recognize that we might have a role here, too. And, of course, I think that Vermont can be very helpful in the fact that it is a small State. They can do some things. They can do some experimenting and all of that, and then maybe we can benefit from it on a national kind of scale.

So, thank you so much for coming. Thank all of you for your testimony. And here again, we will be talking as the days and months go along.

Thank you so much.

I would like to welcome our second panel.

As with the first panel, it is our committee policy that all witnesses are sworn in.

So please rise and raise your right hands.

[Witnesses sworn.]

Mr. TOWNS. Let the record reflect that they all have answered in the affirmative.

Let me begin by asking Kathy Alsbrooks, the Federal Government accountant director for the LaserCard Corp., which currently produces green cards and laser visa cards for the U.S. Government.

And then of course after that we have Neville Pattinson, who is the vice president for business development and Government affairs at Gemalto Corp., and he is representing the Secure ID Coalition.

And of course Mr. Stager is executive vice president at the Digimarc Corp., representing the Document Security Alliance.

So, Ms. Alsbrooks, why don't you proceed?

STATEMENTS OF KATHRYN K. ALSBROOKS, DIRECTOR, U.S. FEDERAL PROGRAMS, LASERCARD CORP.; NEVILLE PATTINSON, VICE PRESIDENT, GEMALTO, INC., REPRESENTING THE SECURE ID COALITION; AND REED STAGER, DIGIMARC CORP., REPRESENTING THE DOCUMENT SECURITY ALLIANCE

STATEMENT OF KATHRYN K. ALSBROOKS

Ms. ALSBROOKS. Thank you, Chairman Towns and Ranking Member Bilbray, and I thank you for the opportunity to appear before you today to discuss LaserCard's role in secure ID programs currently underway and our experience in addressing the challenge in how to make a secure, tamper proof ID card, one that delivers both biometric ID verification and fulfills today's need for visual, reliable inspection, a Flash Pass, when automatic authentication is not available.

LaserCard is a publicly held U.S. company. We are headquartered in Mountain View, CA. For over 20 years, we have been an industry leader conducting research, development and manufacture of highly secure, multi-biometric identity cards.

Today my remarks will focus on the visual and physical security of ID cards which utilize optical memory card technology.

The technology is deployed today in the Green Card, the U.S. Permanent Resident Card, issued by the Department of Homeland

Security, the Border Crossing Card or Laser Visa issued by the State Department. Mexican citizens who frequently cross the U.S. border carry these cards. The Canadian Permanent Resident Card issued by Citizenship and Immigration Canada; the Italian National ID Card and Foreign Resident Card, both issued by the Italian Ministry of Interior, and the Saudi National ID Card issued by the Saudi Ministry of Interior.

More than 30 million of these cards have been issued to date.

The preeminence of optical memory in North American ID security is reflected in these two facts: First, according to US-VISIT stats, the roughly 24 million optical cards in circulation in the Western Hemisphere represent almost 80 percent of all U.S. land border entries by foreign nationals.

And most important, the data security of the optical memory card has never been compromised. In over 15 years of deployment, the data security cards have never been compromised.

To meet the requirements of the Western Hemisphere Travel Initiative and in accord with the recommendations of the 9/11 Commission, LaserCard has developed the LaserPass, which combines unbeatable visual security of optical memory with the facilitation advantages of RFID.

In today's world of advanced machine readable technologies, including our own, why do we maintain a constant focus on visual security as a fundamental requirement?

That answer is simple: Today, visual inspection of ID cards is the norm. The implementation of a comprehensive infrastructure to machine read and authenticate ID documents is a huge undertaking. In fact, Customs and Border Protection officials have stated that RFID readers will only be installed at 39 of the roughly 150 U.S. land ports of entry.

Clearly, visual inspection will remain an essential border entry inspection procedure for the foreseeable future. The more successful the deployments of the Western Hemisphere travel cards, including the PASSport Card, the Border Crossing Card, and the Nexus-Sentri and FAST card, the more widely they will be accepted as the de facto means for establishing identity in flash pass scenarios like airline check-in, airport security and boarding, employment eligibility, provision of government service, banking and building entry.

But, even more importantly, some of these cards will serve to confirm identity as a U.S. citizen.

For all of these reasons and more, the very highest level of virtual security in the Western Hemisphere travel cards is absolutely essential.

Optical memory is, in fact, unique among all advanced ID card technologies in being able to fully meet these needs. The technology incorporates a variety of easily verified visual security features. They support authentication of the card itself, and they offer verification of the card holder's identity. These features are literally tamper proof. They cannot be altered. And they serve to confirm information printed on the face of the card, including the digital photograph and biographical data.

For law enforcement and secondary inspection purposes, optical security incorporates covert security features and forensic security

features supporting suspect document laboratory inspection and expert testimony in criminal proceedings. This unique layering and blending of overt, covert and forensic features in the same media provides an unequaled level of counterfeit resistance.

And finally, optical security also delivers an individually personalized high definition embedded hologram, which shows the card holder's digital photograph and biographical information. This important feature renders each individual piece of optical memory physically and visually unique. This imposes an exceptional barrier in the path of the mass counterfeiter. Most traditional security features are routinely copied or simulated by counterfeiters. Forensic document experts strongly advise card issuers not to rely on a limited selection of security features alone for counterfeit and tamper resistance.

As I described earlier, optical security provides intrinsic layering of security features. The embedded hologram permanently captures the other relevant information from the face of the card and, used in combination with RFID, results in a tamper proof RFID card like that required for implementation of the Western Hemisphere Travel Initiative.

In closing, I hope to leave you with this: Optical card technology is proven. The digital security has never been compromised, and it is physically, literally tamper proof.

Thank you again for this opportunity to speak. I look forward to taking your questions.

With your permission, I have samples of all of these various cards which I have referred to. You can see for yourself what I am talking about after the proceedings. I would be happy for you to look at them.

I have also brought examples of counterfeits of these cards and a demonstration of counterfeit techniques that I would be happy to show you personally, probably not in a public forum.

[The prepared statement of Ms. Alsbrooks follows:]

WRITTEN TESTIMONY OF KATHRYN K. ALSBROOKS
DIRECTOR, US FEDERAL PROGRAMS
LaserCard CORPORATION

Before the U.S. House of Representatives Committee on Oversight and Government Reform, Subcommittee on Government Management, Organization and Procurement

Thursday, October, 18, 2007 2:00 p.m.
Rayburn House Office Building Room 2247

Chairman Towns, Ranking Member Bilbray, and other distinguished members of the subcommittee – I thank you for the opportunity to appear before you today to discuss LaserCard's role in secure ID programs currently underway and our experience in addressing the challenge of "how to make a secure, tamper-proof ID card" – one that delivers both automatic biometric ID verification *and* fulfills today's need for reliable visual inspection – that is, use as a "Flash Pass" - when automatic authentication is not available.

LaserCard Corporation:
LaserCard is a publicly held US company headquartered in Mountain View, California. For 20 years we have been an industry leader; conducting research, development and manufacture of highly secure, multi-biometric identity and credentialing technologies.

While LaserCard's optical memory card fully addresses the needs across a spectrum of ID application requirements, today, I will focus my remarks on visual and physical security of ID cards utilizing LaserCard's optical memory technology.

The technology is deployed today in the following national-level secure ID applications:

a) The U.S. Permanent Resident Card "Green Card" issued by U.S. Department of Homeland Security.
b) The "Laser Visa" Border Crossing Card issued by U.S. Department of State to screened Mexican citizens who frequently cross the border into the United States.
c) The Canadian Permanent Resident Card issued by Citizenship and Immigration Canada.
d) The Italian Citizen ID Card and Foreign Resident Card, both issued by the Italian Ministry of Interior.
e) And the Saudi National ID Card issued by the Saudi Ministry of Interior.

More than 30 million of these cards have been issued to date. The pre-eminence of optical memory in North American ID security is reflected in these two facts:

First, according to statistics published by US-VISIT, the roughly 20 million optical cards in circulation in the Western Hemisphere represent almost 80% of all US land border entries by foreign nationals.
Second, in over 15 years of use, the digital data security of the optical memory card has never been compromised.

LaserCard has also supplied the U.S. Department of Homeland Security with more than 1,000 Biometric Verification Systems which are used at Ports of Entry to automatically authenticate these cards and, where appropriate, verify the cardholder's identity with fingerprint biometrics.

Western Hemisphere Travel Initiative
To meet the requirements of the Western Hemisphere Travel Initiative (WHTI) - LaserCard has developed the polycarbonate-based LaserPass, which combines the convenience and facilitation advantages of RFID with the unbeatable visual security of optical memory.

In this world of advanced machine readable technologies – including our own - why do we maintain our constant focus on visual security as a fundamental requirement? The answer is simple: today, visual inspection of ID cards is *the norm*. The implementation of comprehensive infrastructures to machine-read and authenticate ID documents is a huge undertaking – indeed, Customs and Border Protection officials have stated that RFID readers will be installed at only 39 land Ports of Entry. Clearly, visual inspection will remain an essential border entry procedure for the foreseeable future.

Secondary Uses of WHTI cards – Establishing Identity: The more successful the WHTI card deployments (including the PASSport Card, Border Crossing Card, Nexus-Sentri & FAST) the more widely they will be accepted, requested and inspected as the *de facto* means for establishing identity in "flash pass" scenarios, such as airline check-in, airport security, and boarding, employment eligibility, building entry, provision of government services, and banking. And, let's make no mistake here – some of these cards will confirm US Citizenship. An easily copied document will become the counterfeiter's product of choice.
For all these reasons, the highest level of visual security in the WHTI cards is absolutely essential.

Document Security

Document security requirements include:
- Ease of visual authentication,
- Strong resistance to counterfeiting and tampering, and
- Certainty of automatic authentication.

Visual Authentication
Today, visual inspection of identity documents is the norm. The implementation of a government wide infrastructure to authenticate and read an ID card is an enormous undertaking. Given that issuance of new ID cards to millions of cardholders will take years, visual inspection will remain with us at least in the interim. The more successful the program is, the more widely will the card be accepted, requested and inspected as the *de facto* means of ID. In such a situation ease of visual authentication is essential.

Optical memory is unique among all advanced ID card technologies in being able to fully meet the needs of today's reality - visual inspection - and provide a transition to tomorrow's environment of fully automatic authentication and transactions. And optical memory supports this transition while preserving the highest level of security. In addition to storing digital data in a highly secure manner, optical memory incorporates easily verified visual security features that support authentication of the card *and* verification of the card holder's information and identity. These features *cannot* be altered and serve to confirm other information visible on the card.

Additionally, optical memory can include covert features (requiring a simple magnifier) supporting second level verification, and forensic features supporting laboratory inspection and criminal investigation. This layering and blending of overt, covert and forensic features provides progressive, hierarchical steps in the visual authentication process and an unequalled level of counterfeit resistance.

Counterfeit and Tamper Resistance
Typical criminal attacks on ID documents include the production of "look-alikes" or the altering of genuinely issued documents to another identity, e.g., by photo or image substitution.

Forensic experts strongly advise card and document issuers not to rely on one security feature alone for counterfeit and tamper resistance. They generally favor a "layers on the onion" approach where a combination of features collectively raises the hurdle for criminals seeking to compromise the system. As described above, optical memory provides an intrinsic and unique layering of security features - overt, covert and forensic - combined in a physically unalterable medium to provide certain visual authentication.

Added to this, digital data stored on optical memory *cannot* be altered. This is in stark contrast to inherently erasable storage media. The best-case result of a successful attack on erasable memory (i.e., the attack is detected) is likely to be the enormous logistical and cost burden of replacing all issued cards. The worst case - where the attack may not be detected for a period of time - can result in a catastrophic security breach.

It is worth restating at this point: Optical memory is non-erasable; *its stored data cannot be fraudulently altered.*

In many jurisdictions, information stored on such optical storage media is accepted as evidence in criminal proceedings. The optical memory's ability to store a complete audit trail or history of events in the card's life supports the testimony of forensic experts in counterfeiting and forgery prosecutions. No erasable memory form can comply with this requirement.

Automatic Authentication
Inherently erasable card memory generally needs the support of on-line verification as a defense against criminal attacks. This can include the need for Public Key Infrastructure

(PKI), a complex, costly means of authenticating the card and its transactions. In addition, dependence on on-line functionality may represent an unacceptable risk since the network, as the principal target of hackers (whether mischievous, criminal or terrorist in their intent), potentially becomes a single point of failure.

Optical memory has the advantage of not requiring PKI *and* it can be used securely off-line, obviating the need for a high-cost, totally ubiquitous network infrastructure. Additionally, even in a traditional on-line environment when networks slow down due to overload (or go down due to failure or malicious attack), optical memory can still run securely off-line, maintaining the functionality and integrity of the system.

It is also worth considering that the optical memory acts as a robust back-up to erasable memory which may be accidentally or deliberately erased or corrupted by electromagnetic forces.

Identity Verification

Biometrics
The only way to reliably verify an established identity is through the use of biometrics. While debate continues about which is the most effective, reliable and secure biometric method, it is clear that not all inspection authorities and government agencies will use one and the same biometric technology. This introduces the need to accommodate multiple biometrics and to assure transportability of the data used for ID verification. The use of multiple biometrics, e.g., face and fingerprint, can enhance security where they are used in combination or at random.

Thus the ultimate key to efficiently and effectively verifying a person's identity in multiple agency settings is to provide portability of multiple biometrics.

Whatever biometrics are used, it is very important to be sure that this data cannot be altered to coincide with an impostor's identity. Ultimate surety rests in a memory form than cannot be fraudulently altered.

Transportability
Optical memory has a significant advantage here in that it can store effectively any and all biometric data likely to be used while other memory forms are limited in capacity and flexibility. Not only can optical memory store any number of biometric templates, it also easily accommodates the storage of the original images, such as fingerprints and face, as recommended by NIST and other bodies for transportability of biometrics across system boundaries.

The storage of original images requires a significant memory capacity and, today, the only available proven, secure and durable card technology with sufficient capacity is optical memory.

Other Considerations

Future proofing
Without question, any card solution adopted for government-wide and long-term programs must be as "future-proof" as possible. Only optical memory among all card technologies has the capacity and updateable storage to handle any unforeseen eventualities *without the need to re-issue the card.*

Thus program designers are not constrained to foresee every use of the card from Day One and have the comfort of knowing that the optical memory's "scalable" storage can comfortably accommodate any upgrades, updates and additions through time.

Protection of Privacy
Optical memory's capacity to securely store personal information allows the cardholder to volunteer information on the card, under the principle of "informed consent", by deliberately handing the card over or inserting it into a card slot.

Optical memory cannot be remotely interrogated by radio frequency technologies.

Mr. TOWNS. Thank you very much.
Mr. Pattinson.

STATEMENT OF NEVILLE PATTINSON

Mr. PATTINSON. Good afternoon. Thank you for including me on behalf of the Secure ID Coalition on this panel to discuss the increasingly important issue of identity management and technology for secure identity documents.

For the record, I must offer a disclosure. I presently serve on the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. Nothing I say here today represents the views of that committee or the Department of Homeland Security.

The Secure ID Coalition is an affiliation of companies providing digital security solutions for identification of documents. Our mission is to promote the understanding and appropriate use of identity technology that achieves enhanced security for ID management systems while maintaining user privacy. It is critical that any document used for identification of a person must incorporate the highest levels of securities and features that protect personal privacy.

Our coalition is very concerned with the proposed adoption of RFID technology into the ID documents such as the WHTI PASS card or Enhanced Driver's License.

My company, Gemalto, is a member of the Security ID Coalition and is a leader in digital security with operations in about 100 countries with 10,000 employees, including 1,500 R&D engineers. More than a billion people worldwide use the company's products and services for a variety of operations, including secure identity documents.

The smart cards have been adopted and deployed in many important government programs around the world. In the United States, Gemalto supplies smart card technology to the Department of Defense's Common Access Card program, to agencies deploying HSPD–12 compliant PIV cards, and we supply to the Department of State through the Government Printing Office electronic passport covers.

So what is a smart card and what can it do for securing somebody's identity?

Put simply, smart card technology consists of a sophisticated electronic computer chip embedded in plastic card technology. The chip has an operating system which provides the features and functions for particular applications. The success of smart card technology is in its ability to provide strong security and privacy protections to each individual in a convenient form.

You may consider the computer chip as an electronic security agent representing the issuer of the ID in the hands of the user. The chip security and communications protocol ensure communication and privacy. Some cards communicate either directly through contact or to written devices or over short-range wireless in contactless mode. Whatever method used, in a secure smart ID card, the underlying security ensures both electronic document authentication and user authentication for transacting any credential information. No other technology can offer these features in a cost-

effective and convenient manner to ensure identity and authentication.

RFID is nowhere capable of the security features of that of the smart card technology. Please do not confuse RFID with smart card technology.

Over the past 6 years, there has been a proliferation of ID programs within the Federal Government. The best programs have been developed and implemented independent of similar work taking place within other agencies.

One of the major failings currently in ID management is that there is no unified policy for identity and credentialing processes or documents, and security and privacy questions are left to interpretation. There is no guidance from an appropriate policy framework and very limited oversight.

In some instances, unrealistic program proposals are proffered without any sense of understanding about technologies available or the best practices and standards for security of the program and the privacy.

Further, the vulnerabilities exist in some cases because there is just pressure to get it done.

Privacy must be accounted for in the design, evaluation and implementation of an identity system. It is for this reason that we are alarmed to understand that even though government programs are required to go through a Privacy Impact Assessment process, in many cases the assessment does not sufficiently address the ID document, and those assessments are started many months after the program is well underway.

ID documents are a special category of documents, which require special consideration. Identity documents, once issued, must attest to the identity of an individual and offer a credential, which can be trusted. If there is a weak chain of trust between the ID document, the individual, and the ability to authenticate the claimed identity, there opens up a vulnerability, which may be exploited.

The consequences of this vulnerability may lead to impersonation or fraudulent use of the credential, which will have significant repercussions to the integrity of the identity system and the asset it is protecting.

Therefore, the more effort taken to ensure that a chain of trust can be established between the ID document presented, the user presenting the ID and the validity of the credential, the more confident we are that the person is who they claim to be and the ID belongs to them.

Where high levels of identification assurance are required, several types of security and authentication technologies are combined together. These can be such things as physical security features that we have heard of, forensic features, machine readable technologies, and electronic authentication technologies.

When considering an identity program, the security document technology features just mentioned are available to address a wide range of these issues. The more features, the harder the document will be able to be counterfeited or misused. However, the inclusion of smart card technology is essential to any true secure identity document as proven in the U.S. Government programs that you have previously heard of.

Any identity program that is established to protect our national security and homeland must incorporate smart card technology. Smart cards are incredibly difficult to tamper with, forge, or clone and provide a deterrent for folks trying to do us harm.

Mr. TOWNS. Can you sum up?

Mr. PATTINSON. Certainly.

We offer three conclusions: Any secure identity document must include a secure authentication feature, electronic. We would ask the subcommittee to consider developing a comprehensive body of work that reviews all standards and technologies associated with identity and evaluate them based on the security needs of our country; and third, we would offer our expertise to look at and review the WHTI PASS Card and EDL-RFID technology and see how we can help that program.

[The prepared statement of Mr. Pattinson follows:]

Testimony of

Neville Pattinson, Vice President Gemalto

On behalf of the Secure ID Coalition

Before the Subcommittee on Government Management,

Organization and Procurement of the

Committee on Oversight and Government Reform

Technology for Secure Identity Documents

October 18, 2007

Good afternoon Chairman Towns and Ranking Member Bilbray. Thank you for including me on behalf of the Secure ID Coalition on this panel to discuss the increasingly important issue of identity management and technology for secure identity documents.

For the record I must offer a disclosure. I presently serve as a special government employee to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee (DPIAC). Nothing I say here today represents the views or opinions of the Committee or the Department of Homeland Security. My views expressed today are those of myself, my employer, Gemalto and the Secure ID Coalition.

This important hearing comes at a critical point in the public policy debate as concerns about border crossing, immigration, homeland security and REAL ID have created demand for secure identity credentials. As part of this testimony I will detail and differentiate technologies used in current ID documents and describe what features are needed to create a secure document that can not be tampered with, forged or cloned.

IT IS CRITICAL THAT ANY DOCUMENT USED FOR IDENTIFICATION OF A PERSON MUST INCORPORATE THE HIGHEST LEVEL OF SECURITY AND FEATURES THAT PROTECT PERSONAL PRIVACY.

The Secure ID Coalition is an affiliation of companies providing digital security solutions for identification documents. Our mission is to promote the understanding and appropriate use of identity technology that achieves enhanced security for ID management systems while maintaining user privacy. Member of our coalition manufacturer many different varieties of ID technologies so, we are uniquely positioned to offer expertise in this area.

My company, Gemalto, is a member of the Secure ID Coalition and is a leader in digital security with operations in about 100 countries and over 10,000 employees including 1,500 R&D engineers. Gemalto provides end-to-end digital security solutions, from the

development of software applications through design and production of secure personal devices, often termed Smart Cards, which incorporate a small highly secure computer chip. Part of our portfolio includes smart ID cards, SIMs, e-passports, and tokens which all help the administration and deployment of identity management services for our customers. More than a billion people worldwide use the company's products and services for telecommunications, financial services, e-government, identity management, multimedia content, digital rights management, IT security, mass transit and many other applications.

Smart ID cards have been adopted and deployed in many important government programs around the world including: driver's licenses, health benefits, border crossing, defense, voting and in some countries national ID cards. In the U.S. Gemalto continues to supply smart card technology to the Department of Defense's Common Access Card program; to agencies rolling out HSPD-12 compliant PIV cards; to the Department of State's electronic-Passport program; we have provided cards to the Transportation Worker Identification Credential (TWIC) program; State Assistance programs such as WIC and Medicaid in Texas are now also using our Smart Cards to prevent fraud and abuse of those benefit programs.

What is a smart card and what can it do for securing somebody's identity? Put simply smart card technology consists of a sophisticated electronic computer chip embedded in a plastic card body. The chip has an operating system which provides the features and functions for a particular application. The success of smart card technology is in it's ability to provide strong security and privacy protections to each individual, in a convenient form. Consider the computer chip as an electronic security agent, representing the issuer of the ID, in the hands of the user. The chip security and communication protocols ensure information security and privacy. Many variations of smart cards exist that are all based on International Standards (ISO 7816 & 14443) and are designed to meet the challenges of each specific application. Some cards communicate either directly (contact) to a reading device or over short range wireless connections (contactless). Whatever method used in a secure smart ID card the underlying security ensures both

electronic document authentication and user authentication before transacting any credential information. No other technology can offer all these features in a cost effective and convenient manner to ensure identity security and authentication.

Over the past six years there has been a proliferation of ID programs within the federal government. In most cases these ID programs are developed and implemented independent of similar work taking place within other agencies; often operating as islands or stove pipes developing and requiring different rules and different technologies for programs that are, for the most part, trying to accomplish the same thing. One of the major failings currently in government ID management and ID programs is that there is no unified policy for identity and credentialing processes or documents. In every case, the decision on how to address security of the system and the document itself and the privacy protections of those to be credentialed in the ID systems, are left up to the agency implementing the program. There is no guidance for an appropriate policy framework and very limited oversight.

Instead of learning from the other agencies or departments' implementation challenges and successes each agency is forced to go it alone and "reinvent the wheel" when they decide or it is mandated that they implement an ID program. In many cases hard working federal employees take the time to research other government uses and understand industry best practices and then use those tools to their advantage to meet their challenge. However, in some instances unrealistic programs proposals are proffered without any sense of understanding about the technologies available or the best practices and standards for security of the program and the privacy of those individuals to be credentialed.

Many ID programs are being implemented because of the need for added security to know who is entering either a government building, military installation, port, computer network or, and I would suggest most important, our country across our borders. In some cases programs are being developed and implemented with security flaws that allow for elementary and easy exploitation. These mistakes are being made because there

is limited understanding about the technologies being suggested and no clear guidelines that have been established as a point of reference. Further the vulnerabilities exist in some cases because there is pressure to "just get it done". Efforts to quickly get a program up and running often lead to short cuts the inevitably undermine the programs goals and objectives.

As much as security is the foundation of the all the new identity programs and the guise under which they are being taken up, privacy plays a central and critical role in any ID program. If users, and in many cases, citizens don't have confidence in the technology they are being issued, then programs will immediately become ineffective. Privacy must be accounted for in the design, evaluation and implementation of any identity system. It is for this reason that we are alarmed to understand even though government programs are required to go through a Privacy Impact Assessment (PIA) process in many cases the assessment does not sufficiently address the ID document and those assessments are started many months after the program is well underway. At that point there is almost no ability or willingness to make design or technology changes that will enhance the privacy of those in the system.

Identity documents are a special category of documents which require special consideration. An identity document once issued must attest to the identity of an individual and offer a credential which can be trusted. The presentation of an identity document is usually in connection with the individual having been enrolled in a program and issued an ID. That same individual is now requesting access to a facility or service bound by the presentation of a particular ID. If there is a weak chain of trust in between the ID document, the individual and the ability to authenticate the claimed identity, there opens up a vulnerability which maybe exploited. The consequences of this vulnerability may lead to the impersonation or fraudulent use of the credential which will have significant repercussions to the integrity of the identity system and the assets it is protecting. . Therefore the more effort taken to ensure that a chain of trust can be established between the ID document presented, the user presenting the ID and the

validity of the credential, the more confident we are that this person is who they claim to be and the ID does belong to them.

To reinforce the chain of trust in an ID system, a number of technologies exist today that are often aggregated together in different combinations to address specific ID system challenges. Where high levels of identification assurance are required several types of security and authentication technologies are combined together. Government issued ID cards today mostly incorporate physical, forensic and electronic document authentication.

Figure 1: Security Features as applied to existing US Government ID programs

	Security Features						
Programs	Physical Security Printing	Basic Access Control	Encryped Comms	Mutual Auth.	MRZ	RF Distance	Electronic PII
e-Passport	Yes	Yes	Yes	Yes	ICAO	4"	Yes
TWIC	Yes		Yes	Yes		4"	Yes
DOD - CAC	Yes		Yes	Yes		4"	Yes
HSPD-12	Yes		Yes	Yes		4"	Yes
PASS Card/EDL(RFID)	Yes		No	No	ICAO	30'	DB Number
REAL ID (proposed)	Expected				Bar Code		

Identity Card Technologies and features may be classified into one of four classes. These classes are;

1. Physical Security features which are used for
    a. Visual document authentication, such as:
        i. Rainbow color shading
        ii. Color changing inks
        iii. Printed security patterns
        iv. Holograms
        v. Optical variable devices
        vi. Laser marked overlays
    b. Secondary document authentication, such as:
        i. Microprinting
        ii. Printed fine line patterns
        iii. Hidden or deliberate error features
        iv. UV inks

v. Infrared reactivity

c. Personal Card holder verification

i. Printed Facial photo

ii. Printed Biographical information

2. Forensic security features for detailed document authentication
    a. Taggants (Unique chemical markers)
    b. Chemical ink composition
    c. Plastic body lamination chemistry
3. Machine readable Identifiers;
    a. Bar codes
    b. Magnetic stripe
    c. Laser stripe
    d. Electronic RFID numbers
    e. Optical Character Recognition
4. Electronic Authentication technology (e.g.Smart Card); used for
    a. Electronic Document authentication
    b. Terminal (external equipment) authentication
    c. Credential authentication.
    d. Card holder authentication
        i. PIN codes
        ii. Biometric matching
    e. Secure, confidential encrypted transmission of information
    f. Perform non-repudiation of cryptographic based transactions
    g. Maintaining privacy and security of credential whilst ensuring vigilant access controls
    h. Exponentially increasing the difficulty to counterfeit the document

When considering an identity program the security document technologies and features just mentioned are available to address a wide range of issues. The more features the harder the document will be to counterfeit or misuse. However, the inclusion of smart card technology is essential to any true secure identity document as proven in U.S.

government programs. Any identity program that is established to protect our national security and homeland must incorporate smart card technology. Smart cards are incredibly difficult to tamper with, forge or clone and, provide a deterrent to those attempting to do us harm. Programs that go forward without secure electronic authentication technologies offer an open invitation to be exploited. Smart cards are cost effective, proven technology that is highly adopted in identity programs to protect assets in the U.S. and around the world.

In conclusion we offer three recommendations to the Subcommittee as they begin to address concerns about identity management programs and look at security of identity documents themselves.

1) We ask the Subcommittee to examine programs used to identify citizens on a government wide basis and ensure that they utilizes the highest levels of document security and include citizen privacy protections.

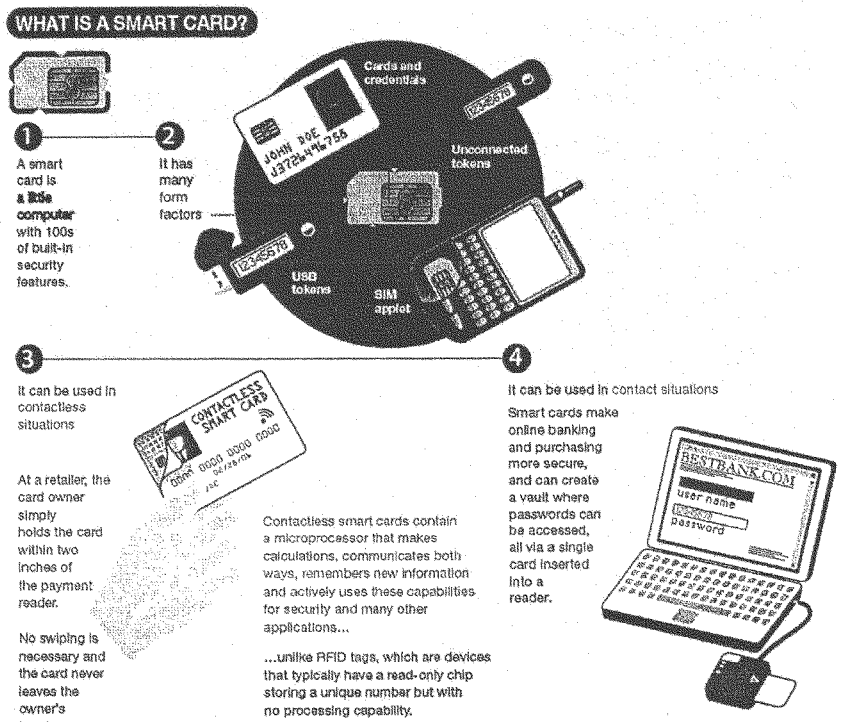
2) Further, we ask the Subcommittee to task the National Institute of Standards and Technologies (NIST) to develop a comprehensive body of work that reviews all standards and technologies associated with identity and evaluate them based on the security needs of our country, and privacy concerns of our citizens. The output of this directive must establish a national standard for identity credentials to which programs must adhere.

3) On a more immediate note we ask that the Subcommittee review the proposed implementation of two U.S. Government identity programs that have raised concerns of the identity industry and privacy community because they fail to meet minimal security best practices and citizen privacy protections. These programs are the proposed WHTI PASS Card and the recently fashioned Enhanced Driver's License, which are both incorporating technologies that do not provide adequate security and privacy protections for our citizens' identities.

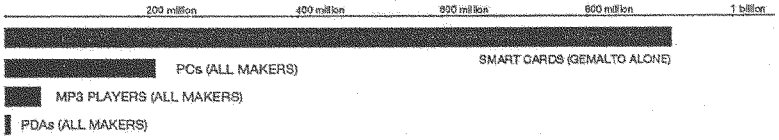
The Secure ID Coalition looks forward to working with the Subcommittee as you begin to address this important and critical issue area of secure identity documents. Please consider our group a resource for expert information and technical assistance. Thank you for your time and I am prepared to answer any questions the Subcommittee might have at this time.

Attachment 1:

Gemalto's microprocessor card technology



Shipments of computing devices, 2005



Source: Gemalto

Attachment 2:

The difference between contactless smart cards & RFID tags

Overview: what happens in RF (radio frequency) communication

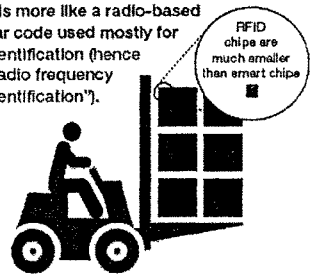
1 When a contactless smart card or an RFID tag passes within range, a reader sends out radio frequency electromagnetic waves.

2 The antenna, tuned to receive these waves, wakes up the chip in the smart card or tag.

3 A wireless communications channel is set up between the reader and the smart card or tag.

The contactless smart card contains a microprocessor, a small but real computer that makes calculations, communicates both ways, remembers new information and actively uses these capabilities for security and many other applications.

RFID tags are devices that typically have a read-only chip that stores a unique number but has no processing capability. It is more like a radio-based bar code used mostly for identification (hence "radio frequency identification").



Characteristics of a contactless card

- Strong security capacities:
  - mutual authentication before providing access to information
  - access can be further protected via PIN or biometric
  - encryption to protect data on card during exchange
  - hardware and software protection to combat attacks or counterfeiting
- Hundreds of security features mean an individual's personal ID, financial details, payment transactions, transit fares or physical access privileges can be safely stored, managed and exchanged
- Read and write memory capacity of 512 bytes and up, with very large memory storage possible
- Short distance data exchange, typically two inches

Source: Gemalto

Characteristics of an RFID tag

- Minimal
  - one-way authentication; card cannot protect itself
  - insufficient storage for biometrics
  - no on-chip calculations of new information
  - relies on static keys
- Single function; used to help machines identify objects to increase efficiency. Example: inventory control
- Small memory (92 bytes); often read-only
- Larger distance data exchange, typically several yards

Because of their more restricted capabilities, RFID tags are generally cheaper.

Attachment 3:

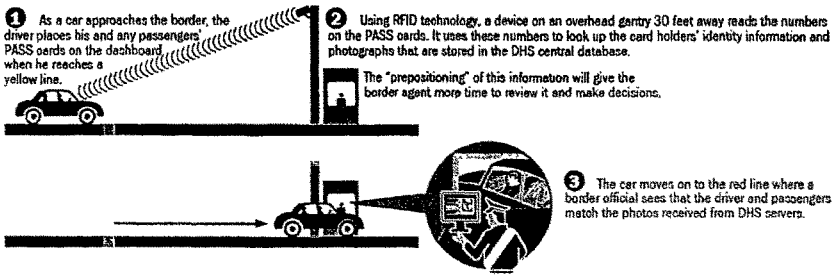
PASS cards: Smart card technology is better than RFID

OVERVIEW

The State Department in conjunction with the Department of Homeland Security is developing PASS cards—a new way for Americans to re-enter the United States from Canada and Mexico.

The purpose is to increase security at the borders, where currently all you need is a driver's license. PASS cards are intended to be a lower cost alternative to passports.

HERE'S ONE PROPOSAL: USING INSECURE RFID TAGS



PROBLEMS WITH THE RFID METHOD

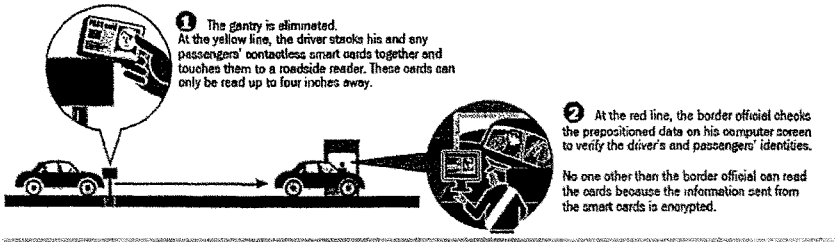
Because RFID technology is designed for product tracking, it's not a technology that protects people's identities...

...it's not secure
Anyone (with an RFID reader) within 30 feet of the traveler can read the card and clone it.

...there are privacy issues
Anyone with a PASS card can easily be identified as an American.

...it won't speed up traffic flow
The PASS card is not like a toll collector tag for your car, where you just roll through; here, all drivers must stop for a visual verification.

A BETTER METHOD: SECURE SMART CARDS



ADVANTAGES WITH THE SMART CARD METHOD

Because a contactless smart card is a small computer with 100s of built-in security features that protect the information in it...

...it's secure
The card encrypts all communications, has a short read range of four inches, and only transmits to a validated reader.

...it protects privacy
No unauthorized person can "read" the information on the card, preserving the citizens' privacy.

...it's just as fast
Information can be prepositioned in the same way as with insecure RFID tags.

Source: Gemalto

Mr. TOWNS. Thank you very much.
Mr. Stager.

STATEMENT OF REED STAGER

Mr. STAGER. Thank you, Chairman Towns, Ranking Member Bilbray, for giving us the opportunity to prevent the views of the Document Security Alliance to this group.

We are here to talk about the technology for secure identity documents, systems and processes.

The Document Security Alliance was created by government agencies, private industry, and academia to identify methods to improve security documents and related security procedures in order to help combat the growing use of counterfeit documents in acts of identity threats and fraud, terrorism, illegal purchase of controlled substances and firearms, illegal immigration, and other criminal acts.

The DSA membership consists of more than a dozen government agencies, including the U.S. Secret Service, the TSA, the Department of Homeland Security, the Social Security Administration, the FBI, the GSA, the FDA, Departments of Treasury and State and the Government Printing Office along with 75 private industry members.

I am also the executive vice president of Digimarc, which is one of DSA's industry members. Digimarc issues more than 60 million identification documents annually, including two-thirds of the driver's licenses in the United States, including the State of Vermont as described by Director Rutledge.

This testimony comments on the need for Federal Government and State governments to adopt end-to-end identity management solutions that address the unique security challenges faced by ID issuers today by incorporating five critical elements of secure ID issues.

This mirrors Director Rutledge's comments. It is not just the credential, it's multiple steps, including data capture, identification verification, secure ID production, secure ID credentials and ID authentication at various points of inspection.

This testimony provides best practices, recommendations on the steps the government needs to take to improve the quality and security of the IDs and Social Security cards and driver's license. Those recommendations are detailed more fully in the written testimony that has been provided.

In order to improve document security, it is important to understand and prove how an applicant is qualified and how a secure ID is issued and used. DSA believes any secure ID infrastructure must include data capture processes, which would be to obtain the applicant's photograph, demographic information, supporting documents, such as breeder documents, which would be Social Security cards, copies of passports, copies of birth certificates, and a digital version of his or her signature and, if necessary, appropriate biometrics such as facial or fingerprint biometrics.

Identification verification would be used to authenticate and validate an applicant's credentials, the breeder documents they present, as well as comparing information against select data bases

such as the Social Security Administration data base as reflected in the REAL ID legislation.

Secure ID production would utilize processes and technologies that enable secure ID issuance. That would include the ensuring of the security of all the materials, the physical facilities and establishing audit and background check procedures for all employees involved with issuing identification documents.

Secure ID credentials would incorporate, as has been discussed earlier today, a layered durable card architecture, which includes both difficult to counterfeit materials with sophisticated laminating and finishing processes as well as a number of overt, covert, and forensic security features.

Many secure documents today have between 12 and 20 security features built into the documents as part of that layered architecture.

Authenticating IDs allows the verification, without infringing on the individual's privacy or taking private information from the document, of the authenticity of a proffered government-issued photo ID, no matter where it was issued at all various points of inspection or transaction, public or private.

One of the areas we cover is the Social Security Administration's card, and that came up earlier today. The audience for that card has traditionally been employers in its use in administering benefits. The card is also used as a breeder document for identifying—establishing identity. However, the DSA's view is that card was never designed for, and should not be considered a secure identity credential.

Mr. BILBRAY. That is an understatement.

Mr. STAGER. Thank you.

As we look at the issue of enhancing security of the Social Security cards, we recommend the following: If the congressional intent is to improve the security of the Social Security card, it is a significant undertaking that will take a number of years. It will take 16 to 20 years to turn over the existing base unless a reissuance process is developed.

The overwhelming majority of misuse and the largest cause of identity theft and fraud is not the use of the credential; it is use of the Social Security number inappropriately.

The immediate focus of security upgrades should be on expanding on-line verification systems allowing law enforcement, employers and others to validate Social Security numbers and names to prevent fraud similar to how the DMV is compared against that data base today.

A number of security features, processes, and best practices would provide additional security, including upgrading to something more than banknote paper, incorporation of a number of variety of practical and cost effective security features as elaborated on in our written testimony.

In any case, if significant upgrades are done, it will be done at significant cost compared to the existing documents.

In terms of driver's licenses, the U.S. driver's license, which has become an increasingly valuable credential as a proof of identity access to most economics transactions, we recommend the five steps I identified earlier be embraced, which is captured in much

of the REAL ID legislation: data capture, verification, secure production, secure credential and authentication.

The 2–D barcodes using the PDF 417 standard is used as the standard overt machine readable technology for carrying data, which is partnered with additional machine readable technologies to enable cross-jurisdictional point of inspection and ID authentication.

The need for implementing this for cross data base verification is important with such systems as the Social Security data base, the Systematic Alien Verification and Entitlements data base, Department of Defense, the Department of State data bases.

This is not necessarily centralized data bases or national ID systems, and the Social Security data base system is an excellent example of how that system can be implemented without impacting citizen privacy.

We also suggest security conscious ID validity periods be established to 5 years.

Mr. TOWNS. Could you sum up?

Mr. STAGER. Yes, I will.

And also that appropriate resources and funding are provided to State DMVs and other government issuing authorities to upgrade the security of their documents and issuance processes.

Document security is a key but often neglected infrastructure element supporting the everyday lives of our citizens. The DSA encourages policymakers to further invest the appropriate resources, time, people and funds to ensure our Nation's identity management system effectively protects our citizens against fraud and identity theft, protect our young people from inappropriate access to restricted products, make the highways and roads safer and protect everyone from additional criminal and terrorist acts.

Thank you for your time.

[The prepared statement of Mr. Stager follows:]

Statement by the Document Security Alliance on Technology for Secure Identity Documents given to the Subcommittee on Government Management, Organization and Procurement of the Committee on Oversight and Government Reform

I. Executive Summary:

This testimony gives an overview of the technical, business process, and public policy recommendations of the Document Security Alliance (DSA) on a host of identity management subjects. This testimony comments on the need for the Federal government and State governments to adopt end-to-end identity management solutions that address the unique security challenges faced by ID issuers today by incorporating five critical elements of secure ID issuance: Data Capture, Identification Verification, Secure ID Production, Secure ID Credentials, and ID Authentication. This testimony provides best practice recommendations on the steps the government needs to take to improve the quality and security of IDs such as Social Security Cards and driver's licenses, and concludes with a number of recommendations. The views expressed in this testimony are the Document Security Alliance's and although experts from government agencies are members of the DSA, no government agency member has endorsed these views on behalf of their agency.

II. Introduction:

On behalf of the Document Security Alliance, I would like to thank Chairman Towns and Ranking Member Bilbray for giving me an opportunity to present the views of the Alliance on technology for secure identity documents, systems and processes.

I am appearing before your Subcommittee to represent the views of the experts of the DSA in the field of secure ID solutions. I currently serve as the Vice Chair of the Government Affairs Committee of the Document Security Alliance (DSA), and I have spoken, testified and worked extensively on document security issues at conferences and with Congressional committees and groups such as the National Council of State Legislatures, American Legislative Exchange Council and a number of U.S. States, and was a key contributor to drafting the SAFE ID Act, which was enacted in 2004.

The Document Security Alliance (DSA) was created by government agencies, private industry and academia to identify methods to improve security documents and related security procedures in order to help combat the growing use of counterfeit documents in acts of identity theft and fraud, terrorism, illegal purchases of controlled substances and firearms, illegal immigration, and other criminal acts. Recognizing the need to continuously improve document security and the issuance process to combat new and existing threats, the DSA is dedicated to work with and educate those responsible for secure document issuance, distribution and use on the value of improving the security and reliability of ID documents. DSA members–in both government and private industry–draw upon the knowledge and detailed technical disciplines of the spectrum of members to accomplish this goal. The group is committed to develop recommendations to appropriate federal and state government agencies, private industry, and policy makers in order to improve the process and procedures surrounding document security.

The DSA membership consists of more than a dozen government agencies and organizations (including the U.S. Secret Service, TSA, DHS, Social Security Administration, FBI, GSA, FDA, and Departments of Treasury and State, and the Government Printing Office), as well as over 75 companies participating in the document security area. Private sector entities and trade associations primarily represent the credentialing industry, including system integrators, card manufacturers, secure printing companies, printer manufacturers; security features producers, and biometric providers.

I am also the Executive Vice President of one of the DSA's industry members, Digimarc, which issues more than 60 million identification documents annually, producing more than 2/3 of all driver licenses issued in the U.S.

III. Worldwide Identity Documents Threats:

Equipment and tools are available today that put counterfeiting ability in the hands of those who previously did not have appropriate graphic or printing skills, making law enforcement's efforts to stop this crime much more difficult. The continuing sophistication of desk top color printers, color laser copiers, high resolution color scanners, imaging and editing software, digital cameras and the exchange of information on the Internet have made document counterfeiting, alteration, and photo substitution able to be performed by the general public. As a result, the ease of obtaining fraudulent identification and phony breeder documents of usable quality has greatly increased as has the need for additional layers of security to be incorporated in the document. The variety of identification document formats has made the visual authentication by humans more difficult and often insufficient to detect fraud. To ensure the ability to discern authentic documents, the use of machine-readable technologies is increasingly necessary.

IV. Elements of a Secure ID System

In order to improve document security it is important understand and improve how an applicant is qualified and how a secure ID is issued and used. DSA believes any secure ID infrastructure must include, at least, the following elements:

Data Capture – Obtain the applicant's photograph, demographic information, supporting documents (such as breeder documents), a digital version of his/her signature, and, if necessary, appropriate biometrics (e.g., facial image or fingerprint).

Identification Verification – Authenticate an applicant's credentials and the breeder documents they present, as well as comparing select information against the issuing authority's databases or other records (e.g., Social Security Administration data). Note that privacy best practices would suggest this be a point-to-point interaction to validate data as in the current Social Security implementation and not a centralized hub or repository where personal information could be accessed.

Secure ID Production – Utilize processes and technologies that enable secure ID issuance.

Secure ID Credentials – Incorporate a layered, durable architecture that includes both difficult-to-counterfeit materials with sophisticated laminating and finishing processes, as well as a number of overt, covert and forensic security features.

Authenticating IDs – Verify – without infringing on an individual's personal privacy – the authenticity of a proffered government-issued photo ID, no matter where it was issued, at all various points of inspection or transaction – public or private sector (e.g., law enforcement, transportation, DMVs, banks or retail).

The DSA has identified a number of best practices that have already been implemented by government issuers of photo IDs in some sectors within the U.S., including –

- Upgrading requirements in obtaining and authenticating "breeder" documents (birth certificates, social security cards, driver licenses, etc.) used in issuing IDs.
- Incorporating new technologies to enable cross-jurisdictional point-of-inspection machine- readable ID authentication – allowing for quick verification of the ID.
- Moving toward issuance of IDs from secure facilities to enable verification processes and provide better control over materials and security features.
- Establishing systems for facial recognition based image identity verification.

- Implementing capabilities for cross database applicant verification (not necessarily centralized databases, information hubs or national IDs systems).
- Shortening issuance and validity periods (e.g., five years) to ensure accurate records and enable security feature renewal/upgrade.
- Providing appropriate resources, training and equipment to State DMVs and other government issuing authorities to upgrade issuance, authentication and verification processes and incorporate new security features.
- Establishing laws (e.g., SAFE ID Act) to provide law enforcement with tools to combat ID counterfeiting.

V. Identity Credential Security:

Documents and cards may be secured in a number of ways including the use of various features or devices:

- Printing – such as deliberate errors and flaws, non-standard print fonts, background printing patterns, microprinting, rainbow printing, anti-copy features, and hidden images or message.
- Inks – such as chemically reactive, infrared and ultraviolet fluorescent, color shifting, photochromatic, thermocromatic, metallic, and many more.
- Substrate inclusion – such as embedding features like threads and fibers, taggent and/or markers in materials, controlled response to UV light, core inclusion, bonding materials, and opacity marks.
- Optically variable devices – such as holograms, color shifting films, color shifting inks, liquid crystals, transparent and metallic features.
- Additional features – such as biometric characteristics, embedded images, security laminates, digital and visual watermarks, laser-engraved or perforated features, retroreflective features, tactile features, tactile features, machine-readable technologies, and many more.

Security features and devices protect documents and assist in proving document authenticity and/or tamper-evidence at three levels of inspection (some security features protect the document in more than one category or Level):

- Overt (Level 1) – this type of device supports inspection and examination without tools or aids that involves easily identifiable visual (naked eye) or tactile (touch) features.
- Covert (Level 2) – this type of device supports inspection and examination requiring the use of a tool or instrument to discern the feature (i.e., UV light, magnifying glass, machine readable technology reader, scanner).
- Forensic (Level 3) – this type of device is used to prove document genuineness through inspection and examination or destruction requiring the use of expert training and laboratory equipment designed to measure select security features known only to a few often for use in case

preparation by law enforcement and for court use. Closely holding the forensic a secret is also a key.

Security features are used to protect against several types of threats to documents:

- Counterfeit or simulation – the unauthorized copy or reproduction of genuine documents by whatever means.
- Forgery or alteration – the deletion, modification, masking, tampering with biographical data concerning the original or rightful document holder.
- Photo and signature substitution – substitution of an imposter's photograph or signature of the original or rightful document holder.
- Cannibalization – creation of a fraudulent document using components from more than one legitimate document.

Document security features facilitate the task of verification and authentication by officials and inspectors throughout the world, making the task as easy as possible under all practical circumstances and conditions. Before a document's security features are selected, a risk assessment must be performed by each issuing authority appropriate to the environment and to meet and combat known and anticipated security concerns. Documents may then be designed using information and features that are "layered" and "linked" on the document. Layering features and devices means providing various types of security devices on each component used in the construction or assembly of the card or document (e.g., certain features on the core and others on the laminates). Layering security features means the document does not become authentic until all of the components are included at the point of manufacturing. Features are designed to work together in the final document so that one complements another (e.g., overlapping features, overlaying features from various layers) creating conditions of extreme difficulty for a credential to be altered and/or successfully counterfeited. In addition, security features that self-destruct and clearly show evidence of tampering are highly desirable to protect against the alteration of data and the reuse of credential by forgers.

The information on the various elements of the document is linked together by repetition of all or a portion of the data in various human and machine-readable portions. Linking ties one part of the document to another to authenticate and secure the document itself (e.g., a birth date, identifying number, or other variable personalized data may appear in printed fashion as an overt feature - readable by the naked eye - and be repeated in a machine-readable bar codes or covert features that can be automatically read and matched for consistency to help provide authentication as genuine). The criminal counterfeiter and forger are defeated by the multiple and varied features necessary to replicate to construct a document that will pass inspection of all security checks. It becomes cost prohibitive for most fraudsters to overcome all of the techniques and technologies thereby allowing law enforcement to concentrate their resources on the more organized criminals.

The DSA recommends the use of at least a minimum number of security features in each of the overt, covert, and forensic levels designed to combat the risk threats identified for each level for document use.

Machine-Readable Technologies

The key to machine-readable technology is interoperability. In the real world, dependence solely upon visual inspection of a document is not sufficient, just as sole reliance on an automated technology without examining and linking to the document holder would be insufficient. In order for identification documents to work both intra- and inter-jurisdictionally, common technologies with interoperating data elements on all credentials facilitate use. The issues of standardization, vendor independence, the logical transition from legacy systems and methodologies, and the migration paths for evolving technologies must all be considered as part of the machine-readable technology selection. Interoperability of document information is essential in any environment where the receiving party or agency is different from the issuer. Common sets of operating rules must be in place to ensure that documents can be accepted and their authenticity validated. Cost-appropriate technologies that secure the assessed risks and threats are required. Currently, most U.S. driver's licenses use one or more machine-readable features, including two-dimensional (2D) bar codes, digital watermarks and magnetic stripes, with 2D bar codes in use by most jurisdictions. This does not preclude the continued use of any other machine-readable technology already or the addition of others as improvements in technology develop.

V. Securing Social Security Cards: Past, Present, and Recommendations:

The Past

Since 1936, the primary audience for Social Security cards issued by the Social Security Administration (SSA) has been employers. The purpose of the card is to carry a unique identification number assigned to an individual, so that earnings can be accurately tracked and attributed to that individual in anticipation of future benefits. As such, SSA maintains that the primary role of the Social Security Number (SSN) is to accurately report the earnings of people who work in jobs covered under FICA so that social security benefits can be properly paid to them.

Congress has consistently maintained that the SSN card is not an identity document and the SSA recognizes that the SSN card is routinely accepted by outside entities as a breeder document for other identification documents. These entities include or have included:

- State Motor Vehicle Administrations (drivers' licenses)
- The U.S. Department of State (passports)

By the 1980s it was becoming apparent that many non-governmental entities were using the SSN and Social Security card as a personal identifier for individuals. Since October 1983, as required by the Social Security Act, the card is made of banknote paper and incorporates a number of other security features designed to prevent counterfeiting.

- The card is currently printed on an optically dead 90 lb. card stock with high cotton content and randomly placed fluorescent planchettes (multi-colored dots)
- The card is printed on high-speed impact printers producing microscopic breaks in the paper fiber and the ink penetrates the surface
- A chemical stain is present to protect against alterations
- It includes intaglio print on the columns
- A microprinted signature line (repeating the words "Social Security Administration") is on the card face
- A blue tint marbleized pattern printed in erasable ink
- A previous version of the card included a VOID pantograph behind the marble camouflage pattern on the card face
- The back of the card includes a red-fluorescing 9 digit alpha-numeric control number

Recently, the REAL ID legislation mandated that State motor vehicle agencies verify an applicant's SSN but not that the applicant must present the card. DHS has not yet completed their rule making for this provision of the law and they could decide to include a requirement for mandatory presentation of the applicant's Social Security card. So, for the time being a State would be compliant with REAL ID if they asked for an applicant's number and performed a verification of the name/number with the SSA, without seeing the physical card itself. Some States currently require presentation of the physical card and they may therefore capture an image of this and retain the image of the SSN card with the images of the applicant's other breeder documents.

The Present

SSA currently issues approximately 20 million cards annually. This number is not expected to increase appreciably. The current price of a card is about 5 cents. The card is relatively easy to mimic, and some trained inspectors are able to spot fraudulent ones. While the primary threats to the SSN card today involve counterfeits, tampering and false issuance, much of the fraud reported today involves the use of the SSN and not specific attacks on the physical card itself (95% of the identity theft is as the result of obtaining a SSN and name through fraudulent methods, such as internet fraud, telephone solicitations and illicit use of personalized documentation). Many employers are not equipped, empowered, or authorized to assess the authenticity of the card or the legitimacy of the card holder.

Some members of Congress have requested that security improvements be implemented on the card, alleging that the current features are not effective in protecting against counterfeits or enabling employers to determine authenticity for work authorization purposes.

The SSA approached the DSA and requested assistance in developing guidelines concerning a more secure Social Security card. A DSA project team reviewed the current and anticipated security threats faced by the card, the expectations of the SSA, and existing legislation (Intelligence Reform and Terrorism Prevention Act of 2004) regarding improvements to the card in order to develop actionable security recommendations to the SSA.

DSA believes the current card should not be considered as a secure credential. There are too few controls and linkages to the intended card holder to offer confidence in the identification value. There are now 54 versions of the card in circulation. Prior to 1978 many cards were issued without proof of age, identity, or immigration status. Large numbers of cards issued pre-1983 are versions without counterfeit, alteration, or tamper-resistant and tamper-evident security features.

Today, to obtain a SSN and card, applicants fill out an application and submit evidence of their age, identity, and citizenship status or lawful immigration status. Non-citizens must provide DHS documentation authorizing them to work in the United States or provide proof of a valid non-work reason for needing a SSN, such as receipt of federal benefits. Applicants age 12 or over are required to have an in-person interview and explain why they never obtained a SSN before. The SSA's 'Enumeration at Birth program' allows parents to obtain a SSN for newborn babies through the hospital during the birth registration process. Applicant information is transmitted through the State to SSA, and a SSN and card are issued.

When an individual's Social Security card is lost or mutilated or the individual reports changes to information contained in SSA's records (such as a legal name change after marriage), SSA issues a replacement card. However, unlike the process for issuing original cards, SSA does not verify the citizenship of individuals who indicate to SSA that they were born in the United States, as long as the citizenship information they previously provided to SSA supports their assertion. As a result, the process for issuing replacement cards may not provide for the cards to be reliable proof of the number holder's entitlement to work in the United States.

Today there are three types of Social Security cards issued:

- Allowing unrestricted work – U.S. citizens and those lawfully permitted who have DHS permission to work

- Not valid for employment – non-citizens who do not have DHS permission to work and state or local laws or a federally funded benefit program require a SSN
- Valid for work only with DHS (INS) authorization – non-citizens who have DHS (formerly INS) permission to work temporarily in the U.S.

Current Attack Data

Most allegations of fraud come from the SSA, law enforcement and the public.

- 81% Identity Theft – Contacts from victims alleging others were using their SSN for unlawful purposes.

Identity theft allegations were further examined to identify the types of activity reported. These were:

- Credit – Use of the SSN to obtain credit cards
- Work – Use of the SSN or card to obtain work, permits or licenses
- Services – Use of the SSN to obtain phone, utilities or cable television
- Benefits – Use the SSN to fraudulently obtain: supplemental Income, disability insurance, workers comp, unemployment, welfare, and tax refunds
- Banking – Use the SSN to open a bank account
- Multiple Identities – Use the number or card to create multiple identities. This activity is presumed to be indicative of future unlawful activity
- Loans – Use of the SSN to obtain a loan under the legitimate card holder ID and not that of the perpetrator
- Child Support – Use of a fraudulent SSN to avoid making mandated support payments
- Avoid Identification – Use of a fraudulent SSN to avoid identification by law enforcement
- Misc. – Unknown use of the SSN by the perpetrator

Discussions with federal law enforcement indicate that most of the counterfeit cards obtained are a result of counterfeit plant suppressions. There are two types of document plants, one that will sell a 'wallet' containing various documents, such as a driver's license, credit card, Social Security card and proof of insurance and the second that specializes in illegal immigrant documentation, such as resident alien cards, driver's licenses, Social Security cards and visas.

Card Consolidation & Replacement

Re-designing security for new cards has an immediate impact only upon new cards issued and those lost, stolen or re-issued. The balance would require approximately 16-18 years evolving into regular use. For new security features to be most effective, a complete re-issuance of cards would be necessary. Yet DSA recognizes the significant costs and impact associated with implementing such a program.

A plan might be devised to replace some card-types based on the estimated number of these cards in circulation combined with the age range of the card

holders. Specifically, those card holders with card-types issued prior to 1983 (without significant security features) and born, say, after 1952 (those between the ages of 25 and 55, who have not been re-issued a newer card-type) might be re-issued with the new card format. Additionally, since there would need to be public education on the re-issuance, it may be easier to explain reissuing cards to younger people rather than to the older card holders.

The DSA team also considered periodic re-issuance of the Social Security card as part of an ongoing process. It was noted that the longevity of the card inherently detracts from the ability to adapt to ever-changing security threats. Reducing the validity period of the card allows for security advances to be added to the card as circumstances require, and the periodic consolidation of card formats for easier recognition. Yet periodic card replacement would likely require additional funding and the development of processes not currently in place.

Education

Education for the issuers and users of a secured item is probably the single most powerful security technique available. Currently with 54 valid designs of Social Security cards in circulation, it is difficult to think of how an employer (motor vehicle clerk, etc.) could, in a short period of time, adjudicate a document presented to them. A secured web site could illustrate two or three overt security features present on the particular card type that could more easily be checked by the employer (inspector) at that time. The site would also give the SSA an opportunity to inform employers of actions that can be taken and the appropriate parties to contact upon receipt of counterfeit card. Requiring employers and/or their employees to register and log-on to this secured site would give SSA the ability to electronically monitor and audit this system.

Recommendations

Given the multitude of security technologies available, and the wide range of costs, placement and effectiveness of those technologies, some might question why one or more available security features were not recommended. Further, the specific choices of technologies are sometimes subjective and can be vulnerable to challenges by individuals with differing views. It is understood that ongoing changes in legislation, increased cost, Congressional appropriations, and technological advances may directly impact the recommendations provided herein.

The goals of the DSA team were several in their evaluation and included:

- Allowing employers to more easily ascertain, without considerable additional costs, card legitimacy
- Features visible to the naked eye were important
- The SS card is not an identity card
- Assume that the federal statutes will continue to require banknote paper.
- No major funding was provided for any increase in SS Card security

- New cards will likely not be reissued to the universe of all 300 million current number holders (more likely only to those requesting originals or replacements)

If it is the intent for the Social Security card to be relied upon as a credential to help establish individuals' identities, more serious consideration of how to enable significant upgrades to the security of the card will be required. The DSA project team focused its efforts on providing a set of recommendations that are neutral in respect to potential vendors, robust, cost-conscious and actionable. The following recommendations, considered in combination, create a version of the Social Security card that is better protected against the threats it faces today and for its continued use in employee verification. In no particular order, the recommendation summary is:

The continued use of:
• Chemical protection
• Both intaglio and offset print technologies
• A manufacturer's control number
• Card production by a security printer
• A microprinted signature line
• Impact as the source of variable print
• Optically dull or dead paper

The removal of:
• Planchettes

The addition of:
• The concurrent introduction of all implemented changes to the card
• Replacing as many versions of the Social Security card as possible with the improved security version
• A hidden message pantograph (for copying protection)
• A strong overt security feature
• Intentional imperfections
• Variable height microprinting
• Slight changes in screen tint
• Ink protection of variable data
• Year of birth and date of issue
• A personalized control number
• Auditing of security protocols
• A signature line for parent or guardian
• Expanded educational content for employers
• Expansion of the SSA website
• Ongoing threat assessments

In addition to the recommendations submitted above, there were a number of recommendations that warranted mentioning, but were outside the interpreted scope of the project. These are:
• Requesting a moratorium on the use of the full SSN on documentation
• An expansion of the SSA's on-line verification system
• An integration of the SSA's on-line verification system with law enforcement databases
• The inclusion of the card control number on IRS and other federal forms where the number is used

VI. Driver's Licenses

Driver's licenses and ID documents issued by motor vehicle agencies are used throughout North America and the world as a "right-of-access". That is, the DL/ID document is used to board airlines, to enter buildings, and to establish identity by government and financial institutions, by corporations, retail, and many other agencies charged with maintaining security and the identification of individuals. One of the greatest uses of the driver's license is to identify citizens party to a commercial transaction, and therefore, a key requirement is to protect citizens from identity theft and fraud. In addition, the events of 9/11 and the 9/11 Commission's Report leading to legislative changes in how states will issue driver licenses and ID cards in support of Homeland Security have become a major issue and States are still waiting final Rulemaking from DHS to find out what their proposed final requirements will be. DSA, using identification security principles, has recommended some of the following items to help the States and DHS combat identity theft and improve security:

Present Day Driver License Issuance
Standards and rules for card production should be applicable to all three existing production/distribution methods for issuing driver licenses and identification cards; over-the-counter, central, and hybrid issuance systems. While DSA favors central issuance production for its greater security and control value, it recognizes that all forms of issuance can be secured and time must be granted for transitioning from current to future systems.

The DSA recommends the current functional uses of the DL/ID documents must continue to be accommodated. These are: evidence of the privilege to drive, identification of the bearer, age verification, address/residence verification, and automated administrative processing.

Verification, Authentication, and Information Capture Considerations
DSA supports the electronic verification of source document information as required by the REAL ID Act, but suggests to DHS that this must only be required when the electronic systems are available (e.g., SSOLV currently is available and

should be used, but the EVVE, SAVE, and State-to-State systems must be developed), and must take active steps to protect citizen privacy. The current Social Security system is a good example where information can be validated but not retrieved using a point-to-point system without centralized hubs or data repositories that may interject additional privacy risks.

Verification is only one part of a complete validation process. It provides information matching and current status, but does not determine if the document is authentic or tie it to the card holder. DSA endorses all three forms of verification (legitimate document issuance, document authenticity, and rightful-holder) with a solution in all cases to each part.

A comprehensive and continuous training program is recommended to empower verification staff to recognize different types of identification documents. Using currently available automated equipment and machine-readable technologies will greatly help verify that the documents presented are genuine.

Use of biometric technologies (i.e., facial recognition and finger images), PINs, and digital image exchange between jurisdictions can help tie the applicant to the document.

DSA continues to strongly recommend an upgrade in the requirements for the production of and security features of "breeder documents" such as birth certificates, Social Security cards, and other documents commonly used in identification proofing for issuing driver licenses and identification cards (the DSA has also prepared a whitepaper and recommendations on birth certificates which is available upon request).

DSA continues to endorse the electronic scanning and archiving of source documents used to prove individual identification. Images should be captured in a digital format for subsequent use in authorized verification, employee training and monitoring/auditing and investigative purposes.

Validity Period and Durability for Credentials

DSA believes that eight years is too long a time for credential validity. It gives too much time for counterfeiters and forgers to find successful attacks to simulate and alter cards in circulation. As technology improves, the fraudster acquires new tools to perform fraudulent activities that are closer to authentic older credential issuances. Durability is another issue. As credentials naturally deteriorate in appearance due to wear over time, it is far more difficult to differentiate a genuine item from a fraudulent one. It makes the counterfeiter's and forger's job much easier since the quality of their criminal products can be much lower to "pass" inspection and examination. We urge DHS to strongly recommend that the States adhere to a shorter time period than the maximum eight years allowed by the REAL ID Act. We continue to suggest no more than a maximum five-year validity period.

DSA also recommended that document durability and performance standards be initiated that include the use of all appropriate substrate materials and that DHS not prescribe one component security product over another. This would allow the continued compatibility of current personalization equipment now in use for secure card issuance as well as allow the migration to more secure materials developed in the future.

Machine-readable Technology Choice

DSA continues to endorse the use of the 2D bar code known as PDF 417 as a common machine-readable technology to start this program. It is already in use by almost all jurisdictions, is very low cost to apply, and is being used currently to facilitate other automated administrative activities by law enforcement in production of traffic citations and accident reporting systems. As stated before, this is not meant to limit other machine-readable technologies from placement on credentials. It is to standardize on one feature that all credentials will contain, allowing universal interoperability. DSA recommends the information in the bar code that matches the information on the human-readable portion of the item not be encrypted. Rather, laws prohibiting collection and use should be enacted to prevent privacy infringement. To encrypt the data currently being used by motor vehicle and law enforcement agencies to validate and authenticate the information will be counterproductive or will result in encryption key management issues that will raise costs of the system while not materially improving security and privacy. Additional machine-readable technologies are being broadly deployed by the States, such as digital watermarking, which provides an effective, low-cost and covert capability to authenticate and prevent the alteration of IDs, and chip-based features, which are being tested for border crossing applications. Both features should be considered as complementary and in addition to the recommended 2D bar code that the DSA proposes as a standard feature.

Physical Security

DSA has established a set of recommended physical and material security standards and procedures/best practices for consideration. They include such areas as manufacturing, resale, shipping, handling, storage, inventory control, and issuance of components and finished products used for identification documents. Some of the DSA specific recommendations fall into the areas of:

Standards: DSA believes the NASPO-ANSI standards should be met in the design and qualification process of motor vehicle card issuance.

DSA Support

DSA and its member government and corporate alliance have volunteered to work with DHS and other agencies as needs arise in Taskforce Groups and Expert Advisory Working Groups to bring their knowledge and experience to address issues and problems in document security. DSA members represent the current and future suppliers of security documents to a wide range of State and Federal governments and stand ready to provide security counsel as needed.

VI. Public Policy Recommendations:

The DSA was created by government agencies, private industry and academia to identify methods to improve security documents and related security procedures in order to help combat the growing use of counterfeit documents in acts of identity theft and fraud, terrorism, illegal purchases of controlled substances and firearms, illegal immigration, and other criminal acts. The group is committed to develop recommendations to appropriate federal and state government agencies, private industry, and policy makers in order to improve the process and procedures surrounding document security. We encourage policy makers to further invest the appropriate resources – mindshare, time, people, and funds to ensure that our nations' identity management systems become best in class.

DSA encourages Congress to adequately fund the implementation of security initiatives for the driver's license and identification cards issued by the states. The communication of information and the realization of the goal "one driver–one license–one record" are achievable. It is important for not only security, but also highway safety, prevention of identity theft and protection of citizen privacy.

VII. Conclusion:

In conclusion, Chairman Towns, Ranking Member Bilbray, and Members of the Subcommittee, I would like to again thank you for giving the Document Security Alliance this opportunity to present our views on a wide range of document security challenges and solutions. As an alliance, we are dedicated to helping policy makers and government executives improve the security cards, systems, and processes that our nation depends on to help protect its citizens. We take this mission seriously and we hope that our discussion today has helped inform the debate in a positive way.

Mr. TOWNS. Let me thank all of you for your testimony.

Let me raise a question about Social Security. My colleague raised an interesting point there.

With Social Security, doesn't it come down to—Social Security cards come down to cost, because right now the card costs 5 cents each. I guess the question is how much would a secure Social Security cost?

Mr. PATTINSON. How much would a secure card cost?

Ms. ALSBROOKS. Depending on the technology you put on it, anywhere between $3.50 to $10, depending on how many chips you had on it, whether you had RFID on it, whether you had optical, all of the different printing techniques.

Mr. BILBRAY. How long would that technology last?

Ms. ALSBROOKS. Our technology has been out there for 10 years. It is durable. I think the new Western Hemisphere Travel Initiative cards are supposed to have a 10-year durability. I think you can count on a 10-year durability.

Mr. BILBRAY. That is if you carried it.

Ms. ALSBROOKS. Yeah. Not in your shoe but, yeah, in your wallet.

Mr. TOWNS. So this boils down to cost, doesn't it? Isn't this a problem, cost?

Mr. STAGER. Yes. If you looked at a base of Social Security cards of 200 to 300 million multiplied by the numbers just presented, it becomes a very significant cost, and yet the majority of fraud and activity around Social Security cards is also the Social Security number being used as opposed to the credential being presented today.

Mr. TOWNS. What do you say to that, Ms. Alsbrooks?

Ms. ALSBROOKS. Can you ask the question——

Mr. STAGER. If there is 200 to 300 million cards in existence that may have to be replaced at those kind of costs versus 5 cents a card, it becomes a very, very large number for replacing all of those cards.

Mr. TOWNS. We are also talking about security now.

Ms. ALSBROOKS. I mean, yeah, to replace that many cards would be a significant undertaking, but it is numbers. I mean, it just depends on how many production capabilities you have and how fast you can get people enrolled and deployed. But that would take a long time.

Mr. BILBRAY. Can I jump in?

Mr. Stager, you were right. The point is it is the forgery.

When is the last time you showed your Social Security card?

Mr. STAGER. I believe it was in 1976.

Mr. BILBRAY. 1976.

The reason why the card does not have—isn't abused very often is because nobody really asks for them any more because they are not worth the paper they are written on. So we go by an honor system on it.

So in all fairness, we do admit that to say: "Well, the abuse is in use of the number, not the card," kind of misses. It needs to point out that the reason why it's the number is because the card is so—has such lack of validity that even the employers that are required technically to see the card just take a number.

Mr. STAGER. We would agree entirely.

Mr. TOWNS. Reclaiming my time—go ahead.

Mr. STAGER. We would agree that the current situation is that the card is easily counterfeited. It has no real purpose for validity. There is no training available.

We reviewed the 54 different versions of it that are outstanding of it today and the fastest way to increase security of citizens is to focus on on-line verification of information. But we also agree that significant security upgrades, as identified in our document, should be made.

Mr. TOWNS. It's interesting we are having this discussion. Just 2 weeks ago on the floor of the House, Members of Congress were just talking about Social Security. And we asked a question, when is the last time you had a Social Security card. And one guy said 31 years since he's had a card. He knows his number and that's all that matters. You know, he just gives a number and that's it. And the other one said 22 years since he's had a card. And they asked me, and I said I don't remember.

So I think that sort of makes the point that if this is something that we begin to emphasize and stress, and we really are talking about security here, then I think that we could view this very differently, because, like you said, there is no question about it.

If there is anything that you think that we can do here? I want to ask very quickly before I yield to my colleague, what do you think Congress should do? Starting right down the line—other than leave you alone.

Ms. ALSBROOKS. No. I don't think you should do that at all. I think what you are doing here is a great thing for you to become educated on some of the details of the issues so that you can formulate policies that really benefit the taxpayer is a great start.

Mr. TOWNS. Mr. Pattinson.

Mr. PATTINSON. The question of Social Security cards is a challenging one. The life expectancy of that card is the life expectancy of the citizen.

So in putting any technologies together, I don't think any of us have technologies that we would put on the table today that would say would last that length of time. Certainly we have technologies that can last certain spans of time and we——

Mr. TOWNS. How long can you have technology can last for how many years now?

Mr. PATTINSON. We know that chip technologies, plastic technologies we can make them for 10 years as we do in passports and driver's licenses as we do today. Those cards—we can look at different technologies, perhaps we can extend them for longer.

But essentially looking for 50, 60-plus years for life span of a credential is a great challenge to our industry, and what you can ask us to do is: to look at what are the appropriate technologies, be them physical features that can be embedded in a card that will add value to that secure credential so that a citizen can present that at any time and it can be a trusted credential; and I think today that is a good question for your committee to ask industry and challenge us with.

Mr. TOWNS. Thank you.

Mr. STAGER. To answer some of the same questions.

The Document Security Alliance recommends a 5-year validity period more because the challenges that the cards have to resist in terms of attacks have to keep up with the technologies employed. So the technology is constantly changing. The security features are constantly changing, and you want to constantly inject the newest and latest technology into the security cards and enable some of these new capabilities.

In terms of what can be done, one of the biggest resources or one of the biggest questions we see from the States is can you help us with the funding, the resources to help us address the REAL ID requirements? Can you help us with upgrading the security of our credentials? And most importantly, if you do that, how are you enabling the Homeland Security at checkpoint, TSA checkpoints, to actually authenticate it using some of the machine readable features that are being deployed.

Those are some of the steps that we believe could help increase security dramatically and quickly.

Mr. TOWNS. Right.

I yield.

Mr. BILBRAY. Let me go back.

Your 10-year projection or 5-year projection of life span, that is based on it being on your person during that period?

Ms. ALSBROOKS. Yes, sir.

Mr. BILBRAY. What would be the life—I am just getting back to this because I think we are mixing apples and oranges here.

There is a different here between the ID driver's license/border crossing card as opposed to the way the chairman has used his lack of a Social Security card for the last—if it was used, basically put in a file, sat there until we changed jobs, what is the life expectancy there? The data, as far as I know, like CDs, they last for hundreds of years.

Ms. ALSBROOKS. We haven't done any studies to that effect, but it logically follows that if it sat in a file, it would last longer than you or I.

Mr. BILBRAY. Staff informed me like how many million do we reissue each year? 20 million at 5 cents each. Maybe you and I, Mr. Chairman, can be the big fiscal conservatives and be proposing that we just stop the silliness of issuing Social Security cards, that we should issue the number electronically and save the taxpayer and quit playing this sham of—as if this is some kind of a breeder document. The number is a breeder—a number.

And I think that's what we need to clarify, is the fact that I would almost challenge anybody now of saying what good is the American taxpayer getting out of this expenditure for the 1930 technology out there, and does it really do any good for you.

I am like you, I can't even remember—I think I signed up as a lifeguard in 1970 was the last time I showed my document, and I have been employed by government agencies ever since. So it just tells you how little it is done.

Let me just say first of all, the issue of Mr.—Mrs. Alsbrooks, has the optical strip been evaluated by a government entity?

Ms. ALSBROOKS. Yes, sir. Several. None that I could tell you here in a public forum, but I will be happy to tell you after the——

Mr. BILBRAY. OK. Do you have any examples of cards that are being counterfeited?

Ms. ALSBROOKS. I have.

Mr. BILBRAY. Can you give us examples of those kind of fake systems?

Ms. ALSBROOKS. Absolutely. I have cards with me that are attempts at counterfeiting the optical memory stripe, and I think when you examine them, you'll see that they are poor attempts.

And I have also counterfeits with me that would be a real challenge for even trained inspectors to differentiate between the fraud and the real card, and I will be happy to show those to you as well.

Mr. BILBRAY. Mr. Stager, I understand that your company is part of the Digital Watermark Alliance. As far as the Federal credentialing program is concerned, what kind of security benefits are gained with the inclusion of the digital watermarks?

Mr. STAGER. To answer that question I will have to put my company hat on as opposed to my Document Security Alliance hat. So I will do so.

The digital watermark capabilities allow for the authentication of documents using machine readable scanners, handheld devices using a covert set of signaling technology that is embedded in the card. It will be in about half the driver's licenses issued next year. It is in about 50 million driver's licenses already today. So it is another layer of machine readable technology, laser authenticated, as well as tie various elements of the document together: the photograph along with the data, the variable data print on the card, and if you have a chip on the card or a bar code, it helps tie that with the digital data contained in that.

So it really acts as an integrity feature as well as an authentication step.

Mr. BILBRAY. Thank you.

Congressional Daily reported that there's been significant delays in the TWIC programs, that DHS is missing deadlines at issuing the cards, but also the fact there are no readers out there, and then there is the issue of can the chips be broken, fried, how they get into it.

Otherwise, are these readable and are they secure without the readers and if the chips get fried and that sort of thing?

Mr. PATTINSON. The chip program has been going for many years, and I think it is successful to DHS that they are now issuing those chip cards to help protect our ports.

The chip technology in there has been based on the Federal FIPS 201 standard based out of HSPD–12. The credential contained in them has been secured with the chip as well as on the surface of the card.

The extension that the TWIC program took to secure the communications of that credential of the wireless side has been a tremendous addition to that program. I think seeing that TWICs now are being issued and are securing the ports is a great thing.

As far as the security elements that you are concerned there, if any element of the card or the chip is compromised, you have to fall back on your next level of security. So if you had the chip would be compromised or the card would be damaged, one of the other security features has to be present for you to fall back on to

still authenticate the card. Ultimately you are going back to back-in system to verify that this is the credential that person should be presenting and should be accessing a device or service.

It is many layers. It is not just a question if a chip is broken or a card is damaged.

Mr. BILBRAY. That's essential.

One thing I learned when I was running jails or building jails you always wanted to have multiple barriers so that while they may break through one or two, the third one will always catch them, and the same thing with security.

Mr. Chairman, I want to thank the panel for being here. I want to thank you for holding the hearing, and the sad part about it there are questions I have about our national security about IDs, but if it is any indication of where I think we haven't done our due diligence as a nation and the administration hasn't done their due diligence as an administration, there are questions and concerns that I have about securing different facilities in this city and around the country that I cannot ask in public because I think it would compromise security if the facts of the situation were put out to the public.

So I look forward to working with you, and I am very honored to be able to serve as your ranking member on this committee.

Mr. TOWNS. Thank you very much. I appreciate your kind words.

Mr. Pattinson, you don't like the RFID cards.

You heard the last panel. I mean, they say the convenience offsets the privacy concerns. You know, how do you respond to that?

Mr. PATTINSON. Well, Chairman Towns, I think we have to look at the technology of RFID for what it is good for. And, for what it is good for is revolutionizing the supply chain tracking industry, and I think the good things that it is doing there in implementing supply chain efficiencies are outstanding. And that is a very good application of that technology.

What concerns me is its simplicity. I think it is a very small electronic device that is capable of doing one thing, and that is when it is stimulated transmitting a unique number. A unique number stays the same every time it is stimulated.

On that basis, applying it to the use of human identification to me is a concern. There is now another number that can be associated with an individual. So that has ongoing privacy issues.

But more importantly than the privacy issues here—and they are important—that even though they exist, there is security issues. This technology is extremely weak in its feature of its security. It has no operating system. It has no security features that can determine that the document or the device is authentic. It cannot perform any of the features that other sophisticated chip technologies can perform.

So an RFID device being used in a human identification situation is alarming in the basis that it has vulnerabilities. People can now potentially create copies of these devises. They can clone them. They can try and masquerade under somebody else's unique number. These devices are insecure in the form of—of testing that is the original document that was issued to the particular individual.

So RFID on its own I think is inappropriate in the situation.

And DHS has done a lot of effort to look at the document and to look at the RFID to put a sleeve around the device. Now putting a sleeve around the device to me is a recognition of a failure of technology. To have a sleeve around a device that's got RF capability to me is unfortunately a recognition that there is something wrong with—why they have to put the sleeve there in the first place.

Smart card technology as used in all of the PIV programs, HSPD–12s, the electronic process, they didn't have sleeves. This technology is such that it does not require to be protected from illicit stimulation. You have to have protocols and procedures that will wake up the chips appropriately, and the chip will perform a secure operation with its communicating reader and perform a secure transmission of the information.

RFID technology has none of that capability. It has only the ability to transmit a single number.

Mr. TOWNS. You don't like it?

Mr. PATTINSON. Yes. In this application.

Mr. TOWNS. I understand the application of smart cards with chips if you have the readers. But are you going to ask every small business, every police officer, every bank branch to install a reader?

Mr. PATTINSON. I think it's a question of if you create a credential that can be trusted, that includes electronic technology for authentication of an individual, and you put it out there, people will start to adopt it. You don't have to mandate or enforce that all of those entities that you just described has to buy those things. It is entirely optional that they would, but I think to see the benefits when they did install that, they would have a higher level of assurance that they could determine that this was an authentic document and it belonged to the person who was presenting it.

And on that basis, they have a much higher assurance that this isn't somebody who was trying to perform an identity theft.

Mr. BILBRAY. Like the swipe card with the Visa where they went away with the imprint?

Mr. PATTINSON. You mean the PayPass and the various ones from Master Card and Visa today?

Mr. BILBRAY. Yes.

Mr. PATTINSON. They are banking industry's recognition of convenience of providing a radio-frequency based communications, secure communication between the card and the reader for convenience at the transaction point.

Mr. BILBRAY. But that has happened in the last 20 years. Almost all businesses now have slide card technology?

Mr. PATTINSON. You mean just——

Mr. BILBRAY. I mean just for credit cards.

Mr. TOWNS. Mrs. Alsbrooks, I have to ask you, will you respond?

Ms. ALSBROOKS. Our experience with reader deployments has been that they don't materialize as rapidly as we would like to see and you know, you mentioned earlier that the TWIC program has been going for quite a while. There have been difficulties with the readers that they have chosen for various reasons. They will be deploying the readers, and they are studying them now.

But as of now, the TWIC cards are what we refer to as Flash Passes because the readers are not out there to verify them in all of the ports.

As you see, I keep hammering on the issue of a Flash Pass. You know we—all of our machine readable technology as well as secure physical technology, we incorporate either RFID chips in our cards or contact chips in our cards.

Our Saudi National ID program is in partnership with Mr. Pattinson's company, Gemalto, and I have one of my chips on my Saudi card with an optical technology.

But inevitably, reader technology can be disrupted. The power can go out. You can fry the chip. You can break a chip.

This is my very own contact card, common access card. If I take my fingernail like that and do that, that chip is dead. It is never going to work again.

And then I have a Flash Pass. And this card has some significant problems in terms of document security. I could take the hologram off, I could wipe it clean with fingernail polish remover and put my own picture on it, and I can demonstrate some of that to you later.

Ultimately, I think the best secure card will incorporate both the highest level of security of machine readable technology but will also continue to use technologies that have been proven to be very reliable for document security.

You will be able to look at the cards and know that, one, it was issued by the U.S. Government. It wasn't manufactured in someone's garage or by a drug gang, and you will be able to look at the photograph and biographical information in the stripe and know that the front of the card has not been tampered with, that this photo matches this photo and this information matches this information. And that, today, we believe is the most secure Flash Pass you can get.

Mr. TOWNS. Let me thank all three of you for your testimony. You have been very, very helpful in terms of—I really want to thank you for that and to say that we look forward to working with you in the days and months ahead to see in terms of how we might be able to solve some of the problems that we are encountering, because there are some problems as you would readily admit, I am sure. It is going to require working together to be able to bring about the solution, and we look forward to doing that.

Thank you so much for coming. We really appreciate your testimony. The hearing is adjourned.

[Whereupon, at 4 p.m., the subcommittee was adjourned.]

○